DOCUMENT RESUME

ED 320 581 IR 053 178

TITLE	Florida's Information Policy: Problems and Issues in the Information Age.
INSTITUTION	Florida State Legislature, Tallahassee.
PUB DATE	Apr 89
NOTE	273p.; Joint Committee on Information Technology Resources.
PUB TYPE	Information Analyses (070) -- Legal/Legislative/Regulatory Materials (090) -- Reports - Research/Technical (143)
EDRS PRICE	MF01/PC11 Plus Postage.
DESCRIPTORS	*Access to Information; *Computer Software; *Confidential Records; Freedom of Information; Information Dissemination; *Policy Formation; Questionnaires; *Records Management; Surveys
IDENTIFIERS	Computer Security; Florida; *Government Records; *Information Policy

ABSTRACT

This report examines the major issues arising from the impact of information technology on the creation of government information and its storage, processing, and recordkeeping, based on information gathered through a literature search, several mailed questionnaires, and three public hearings. An outline of the background of the information policy debate in Florida includes: a brief history of public records law, general principles of access in Florida, definitions of public records, exemptions, content and format of access, the cost of access, and the enforcement of sanctions. Findings of the study are outlined in nine chapters: (1) Defining Reasonable Access; (2) Security Concerns; (3) Legal Issues Associated with Optical Storage; (4) Dissemination of Public Information; (5) Computer Software Issues; (6) Computer Matching; (7) Fair Information Practices; (8) Technological Impacts on Privacy; and (9) Records Management and Archival Concerns. Conclusions and recommendations for state information policy are outlined in the final section. Appended are the proposed information policy legislation, copies of the questionnaires used in the study, public hearing agendas, and laws and opinions related to the copyright of public software. (65 references) (GL)

****
* Reproductions supplied by EDRS are the best that can be made *
* from the original document. *
****

U.S. DEPARTMENT OF EDUCATION
Office of Educational Research and Improvement
EDUCATIONAL RESOURCES INFORMATION CENTER (ERIC)

X This document has been reproduced as received from the person or organization originating it.

☐ Minor changes have been made to improve reproduction quality.

• Points of view or opinions stated in this document do not necessarily represent official OERI position or policy.

"PERMISSION TO REPRODUCE THIS MATERIAL HAS BEEN GRANTED BY

Edwin A.Levine

TO THE EDUCATIONAL RESOURCES INFORMATION CENTER (ERIC)."

FLORIDA'S INFORMATION POLICY:

PROBLEMS AND ISSUES IN THE INFORMATION AGE

The Florida Legislature
Joint Committee on Information Technology Resources

April 1989

BOB CRAWFORD
President

TOM GUSTAFSON
Speaker

THE FLORIDA LEGISLATURE

JOINT COMMITTEE ON INFORMATION TECHNOLOGY RESOURCES

Senator George Stuart, Jr., Chair
Representative Susan Guber, Vice-Chair

EDWIN A. LEVINE, STAFF DIRECTOR
111 West Madison Street
Room 876
Tallahassee, Florida 32399-1400
Telephone (904) 488-4646

FLORIDA'S INFORMATION POLICY:

PROBLEMS AND ISSUES IN THE INFORMATION AGE

This publication was produced at an annual cost of $1,732.20, or $5.32 per copy, for the purpose of informing members of the Legislature and the public.

April 1989

TABLE OF CONTENTS

	PAGE
EXECUTIVE SUMMARY	1
I. INTRODUCTION	23
Purpose	23
Methodology	23
Organization of Report	24
II. BACKGROUND	26
Brief History of Public Records Law	27
General Principles of Access in Florida	29
Definitions of Public Records	29
Exemptions	31
Content and Format of Access	33
The Cost of Access	35
Enforcement of Sanctions	37
III. FINDINGS	38
CHAPTER 1 - DEFINING REASONABLE ACCESS	38
CHAPTER 2 - SECURITY CONCERNS	54
CHAPTER 3 - LEGAL ISSUES ASSOCIATED WITH OPTICAL STORAGE	64
CHAPTER 4 - DISSEMINATION OF PUBLIC INFORMATION	74
CHAPTER 5 - COMPUTER SOFTWARE ISSUES	83
CHAPTER 6 - COMPUTER MATCHING	97
CHAPTER 7 - FAIR INFORMATION PRACTICES	110
CHAPTER 8 - TECHNOLOGICAL IMPACTS ON PRIVACY	122
CHAPTER 9 - RECORDS MANAGEMENT AND ARCHIVAL CONCERNS	135
IV. CONCLUSIONS AND RECOMMENDATIONS	142
V. REFERENCES	155
VI. APPENDICES	160

00: 5

TABLE OF APPENDICES

APPENDIX A
PROPOSED LEGISLATION

A-1 Information System Disaster Recovery Act

A-2 Voter Protection Act

A-3 Optical Image Record Storage by the Department of State

A-4 Fair Information Practices Act

APPENDIX B
MAILED QUESTIONAIRES

B-1 Access to Automated Public Records

B-1A Response Rate by Respondent Type

B-2 Survey of Computer Matching Activities in State Departments

B-3 Survey of Fair Information Practices Legislation and Computerized Matching Activities in Other States

APPENDIX C
PUBLIC HEARINGS AGENDAS

C-1 January 9, 1989 - Tallahassee

C-2 January 18, 1989 - Ft. Lauderdale

C-3 January 19, 1989 - Orlando

APPENDIX D
LAW AND OPINIONS RELATED TO THE COPYRIGHT OF PUBLIC SOFTWARE

D-1 Chapter 119, Florida Statutes

D-2 Attorney General Opinion 86-94

D-3 Attorney General Opinion 87-1

D-4 Attorney General Opinion 88-23

D-5 Dade County Legal Memorandum regarding Licensing Agreement for County-Generated Software Products

TABLE OF EXHIBITS

PAGE

EXHIBIT 1-1 40
Public Records Custodians Reporting
Some Automation of Records

EXHIBIT 1-2 42
Methods By Which Public Record Custodians
Provide for Inspection of Public Automated
Records

EXHIBIT 4-1 76
Methods by Which Public Record Custodians
Provide Copies of Automated Records

EXHIBIT 6-1 101
State Departments Which Participated in
Computer Matching and Front-End Verification
Activities During 1987-88 Fiscal Year

EXHIBIT 8-1 127
Diagram Showing The Information Sharing
Among Computers

EXECUTIVE SUMMARY

Purpose of Study

The state's information policy consists of a variety of laws and rules that govern how the state and local governments collect, use, store and disseminate information. State and local governments in Florida are increasingly adopting technology as a way to improve their efficiency in record keeping. As more public records are automated, the laws governing them, which were written primarily at a time when most records were paper documents, require review. The purpose of this report is to examine the major issues arising from the impact of technology on government record keeping, and to make recommendations on the state's information policy in response to those impacts.

This report is based on information gathered through a literature search, several mailed questionnaires, and three public hearings. The hearings were held in January 1989 and focused on the issues which had been identified through the earlier research.

Background on the State's Information Policy

The state's information policy is reflected in numerous statutes and administrative rules. Over 120 laws require a report to the Governor, and more than 200 laws require a report to the Legislature. These laws reflect a state policy which encourages open communications and review.

Florida has over 300 laws dealing with various aspects of government records and their management. One of these is the Information Resources Management Act, ss. 282.303-.314, F.S., which

requires statewide planning for information resources management. The law defines information resources management as,

> the planning, budgeting, organizing, directing, training, and control associated with government information. The term encompasses both information itself and the related resources associated with its use.

The centerpiece of the state's information policy, however, is the Public Records Law, Chapter 119, Florida Statutes. Florida, in 1909, enacted one of the first public records laws in the nation. The present revision of the state's policy was adopted in 1975 and reads: "It is the policy of this state that all state, county, and municipal records shall at all times be open for personal inspection by any person."

Access to public records is controlled by five factors: the definition of public records, the number and substance of exemptions, the content and format of access, cost of access, and procedures for enforcement and sanctions for violations. The definition of a public record is broadly defined in Florida to include "any material prepared in connection with official agency business which is intended to perpetuate, communicate, or formalize knowledge of some type." Although there are over 200 specific exemptions to the law, a record is presumed to fall under the law unless an exemption is specified.

Florida makes the right of inspection available to any person regardless of interest, purpose, or use. The court has stated that record custodians do not have to provide access to computerized records in the particular formats which may be requested by the user.

Access to public records includes visual inspection and copying of the records. Fees can be charged for the cost of the copies, which in most cases includes only the actual cost of duplication. Florida

law provides the authority for custodians to provide remote electronic access to the public records and to charge a fee.

When denied access to public records, an individual may institute a civil action to compel compliance. Sanctions for violations of the Public Records Law are provided for both exposing exempted records and willfully and knowingly violating any of its provisions.

Defining Reasonable Access

The majority of government information in Florida is stored electronically. Once automated, records can be accessed in numerous ways. This array of possibilities makes it more difficult to determine what is "reasonable access" and what constitutes an "extensive use" of information technology.

Some innovative public records custodians in Florida and around the country have responded to the opportunities offered by information technology and provide remote electronic access to public records. However, only 20% of the record custodians surveyed by the Committee in 1988 report that they have written policies on access to computerized public records.

Security Concerns

Various Florida laws require record custodians to provide security for public records. Public records custodians face conflicting demands to provide easy access and yet retain a secure system.

When public records systems are first automated, conscious planning for electronic access to those records by the general public

rarely occurs. The networking of different computers increases the exposure of the systems to security risks, since the computers on the network are only as safe as the weakest link.

A high priority security need for the state is the provision of a "hot-site" facility. Such a facility would provide data processing for critical applications in the event of a disaster.

One area of computer security which has received increased attention this past election year is the security of computerized voting systems. Errors and accidents have occurred in computerized elections, both in Florida and around the country.

Legal Issues Associated with Optical Storage

Optical storage is a new technology, and the law is only now beginning to grapple with the issues resulting from its use. Major issues include whether an optically stored image is an original record or a copy, and whether an optically stored image is admissible as evidence in court.

Section 15.16, F.S., authorizes the Department of State to record information by means of electronic data processing and admit into evidence information stored by photography or microphotography. Given the express authorization of admission into court of only certain records, it appears optically stored records are not admissible because they are not expressly mentioned.

As evidenced by various laws authorizing its use, the Florida legislative trend is to accept electronically produced documents as originals. However, no administrative rules exist for the use of such systems. Other states, particularly Texas, have grappled with this

issue, and the federal trend favors the legality of optical storage. Similarly, the private sector is also supporting the use of the new technology.

Dissemination of Public Information

Historically, information dissemination has been a primary function of democratic governments. However, the private sector information industry is rapidly growing and calling into question the government's role in the dissemination of information.

An informed citizenry is a basic requirement of democracy. Florida provides its citizens opportunities to become and stay informed through laws which guarantee open records, open meetings, provide for public libraries as depositories of public documents, and require the printing of annual reports of government programs.

It is, however, often difficult to distinguish what information the government should disseminate on its own versus what it should "contract out" or leave for others to develop and disseminate. Some argue that government must always retain the function of disseminating information, while not restricting others from doing so. To do otherwise, would threaten the concept of an "informed public" and could result in the dissemination of "profitable" data by the private sector, and other information not being made available at all.

Computer Software Issues

The Federal Copyright Act explicitly prohibits the federal government from holding copyright in its works, but does not specify whether state governments may hold copyright in their works. Florida law, in specified instances, permits the state and certain agencies to hold copyrights.

Some local governments in Florida are particularly interested in marketing their internally developed software to partially recoup their software development costs. Existing statutory law, case law, and attorney general opinions indicate that software is a public record and therefore subject to the inspection and copying provisions of Ch. 119, F.S., unless it meets one of the statutory criteria for exemption.

In Florida, it is not unusual for agencies to use two types of software: that which they write and that which they purchase through a licensing agreement. Agency produced software is subject to inspection and copying; purchased software is exempt from inspection and copying. This distinction impacts on the public's ability to know about its government, how it functions, and how certain decisions are made. The exemption status of privately-owned and copyrighted software has been questioned in a court case in California with ramifications for Florida.

If government-produced software were statutorily exempt from the inspection and copying provisions in current law, concerns could be raised about the government competing with private sector software developers.

Fair Information Practices

The federal Privacy Act of 1974 incorporates fair information principles by giving individuals the right to access much of the personal information kept on them by federal agencies, placing limits on disclosure to others, and requiring agencies to keep logs of all disclosures of personal information. It also gives individuals the right to change incorrect information pertaining to them.

An inevitable tension exists between the freedom of information goals and privacy concerns. Ten states have enacted fair information practices legislation, and their implementation experiences have been varied. Although Florida does not have a fair information practices law, the state has codified several components of such laws.

As the technologies for telecommunications, networking, and computer systems integration continue to improve, they greatly increase the ability of government organizations to share information with each other. However, these same advances make it more difficult for individuals to monitor agency information practices, to learn how their records are being used, and to access and amend information on themselves.

Computer Matching

The rapid development of computer technologies has enhanced the ability to match millions of records, and governments' use of computer matching has increased dramatically as a result. Until recently there have been few, if any, controls on matching in the federal and state governments. In October 1988, Public Law 100-503, the Computer Matching and Privacy Protection Act, was enacted which will regulate

matching programs conducted by federal agencies or by other agencies using federal records, including state agencies.

Computer matching occurs frequently among state agencies in Florida. The Committee's survey of state agencies reveals that during the previous year, an estimated total of 18 million records were matched. The use of computerized matching to decrease fraud, abuse, and waste in government programs is stimulated by both improved technology and decreasing program resources.

There is, however, no state statute which regulates computer matching in Florida agencies and consequently no legislative oversight of such activities.

Technological Impacts on Privacy

Concerns exist that a "dossier society" is emerging as both private and public information systems collect and share personal information in increasing amounts. The federal Privacy Act of 1974 places restrictions on the collection, maintenance, use, and dissemination of federal agency records. However, few state laws or policy guidelines govern how personal information is collected and used.

Balancing the privacy of individuals against the information needs of government is increasingly difficult due to the extensive storage of personal information in government computer systems. The U.S. Office of Technology Assessment concluded that federal use of new electronic technologies has eroded the protections of the Privacy Act.

A significant problem is the government's collection of non-essential personal information which becomes subject to public

disclosure. This fact has special relevance for Florida, where the Public Records Law makes virtually all types of personal information subject to public disclosure.

Records Management and Archival Issues

Archival and records management programs were developed to deal with paper records. Although microfilm has become a legal and accepted storage medium, the use of electronic, magnetic, and optical storage media create significant new problems for storage, security, and accession. The increased use of microcomputers, electronic mail, and electronic data interchange (EDI), could result in the loss of the historical record because a paper document may not be produced for others to evaluate, store, or protect.

Issues related to records management in an information age are not unique to Florida. Federal, state, and local governments are all experiencing significant difficulty in preserving their public records.

Florida is rapidly adopting information technology for creating, using, and retaining information. At the state level, total expenditures for information technology have grown from approximately $150 million in FY 1983-84 to approximately $285 million in FY 1987-88. As a percentage of the state budget, information technology expenditures have increased from 1.3% in FY 1983-84 to approximately 1.6% in FY 1987-88. However, unless explicit attention is given to archival issues, the use of technology may erode the ability to preserve our past and promote the retention of useless or irrelevant information.

CONCLUSIONS AND RECOMMENDATIONS

Defining Reasonable Access

Based on the findings regarding access to public records, the following conclusions are drawn:

- Electronic records are accessible in many more ways than are manual records, thus making the record custodians' requirement under Ch. 119, F.S., to provide access to records at "reasonable times" and under "reasonable conditions" more difficult to define.
- As more records are automated there is a need to ensure that meaningful and equitable access to them is maintained.

Therefore, it is recommended that:

1) Public record custodians provide access procedures that keep pace with the technology by: providing access to records through automated as well as non-automated means; providing public access terminals on-site once the majority of their records are automated; and allowing the public to use the database management software available so the public may retrieve the desired information more easily. The Legislature should continue to monitor access policies to determine if statutory changes are required.

- Insufficient attention is paid to access requirements when systems are initially designed.

Therefore, it is recommended that:

2) The Information Resource Commission, subject to available resources, develop a rule on systems design and development that addresses public access requirements for state systems.

- Current laws adequately provide for an alternative form of access, remote electronic access, which has been successfully used by several state agencies and local governments.

Therefore, it is recommended that:

3) The law providing for remote electronic access to records should be retained, subject to the Legislative review required by law.

- Current law allows for inconsistencies in fees charged since each record custodian must decide what is "extensive" use of personnel or information technology resources in determining any special charges for copying. These inconsistencies may reflect the variations which exist in each custodian's situation.

Therefore, it is recommended that:

4) Record custodians continue to be provided, under current law, the flexibility of defining what is "extensive" in their situation. However, record custodians should also establish costing algorithms in writing which accurately reflect the costs they incur and form the basis for their charges.

- Some confusion exists as to the responsibilities of centralized data processing departments in maintaining the records of constitutional officers.

Therefore, it is recommended that:

5) The Secretary of State's Division of Library and Information Services review its existing rules on records management to determine whether further clarifications in this area are needed.

Security Concerns

Based on the findings regarding computer security the following conclusions are drawn:

- The automation of public records presents new security problems for record custodians, particularly with the increased networking of computers.

Therefore, it is recommended that:

6) Agencies include in their budgets for new or improved applications the costs associated with providing the necessary security measures for the applications.

- Records security is too often an afterthought, rather than included as a part of the process of automated systems designs.

Therefore, it is recommended that:

7) The Information Resource Commission, subject to available resources, develop a rule requiring agencies to include security considerations as part of each overall systems design project.

- The existing laws and rules regarding the security of records have provided a good framework for the state agencies. However, funding for computer security has been insufficient to meet the agencies' needs.

Therefore, it is recommended that:

8) Increases in state funding for security of state systems be requested. Agencies, particularly those with data centers, should request funds and positions to perform the Information Security Manager function, as mandated by law since 1984.

9) Funds for a disaster recovery facility should be made available to ensure continued operation of critical applications in the event of an emergency. (Legislation to accomplish the latter is included in the Appendices.)

o Those agencies which provide remote electronic access to records under Ch. 119, F.S., are taking steps to ensure the security of those records.

Therefore, it is recommended that:

10) The State continue its current policy of requiring the custodian to ensure the security of the records in a remote electronic access environment and continue to allow the custodian to determine the best method for security in each case.

o The increased use of computerized elections systems intensifies the security concerns for those records, since they are vulnerable to security risks of fraud and error.

Therefore, it is recommended that:

11) The elections laws be amended to:

a) Provide that a manual recount of computerized votes is permissible.

b) Provide authority for the Department of State to develop elections software (as the City of Los Angeles has done) for use by each jurisdiction desiring to do so.

c) Require electronic voting systems to have an audit trail.

d) Require that any vendor which gets approval from the Secretary of State to sell their vote-counting software in Florida must place the source code for their software in escrow.

e) Require the Division of Elections to establish ballot card standards.

f) Require each supervisor of elections to conduct independent audit of their system procedures and software performed on a periodic basis.

g) Provide authority for the Department of State to provide technical assistance to local jurisdictions.

It is further recommended that:

12) Increased funding be provided to the Division of Elections to strengthen its ability to certify electronic voting systems and provide better support to supervisors of elections.

13) The Division of Elections:

a) Encourage the phase-out of the use of mechanical lever machines.

b) Strongly encourage, or begin a phasing-in process for, digitizing signatures and bar coding voter I.D. numbers as a way of enhancing the integrity of voting records and speeding up the signature verification process.

c) Require that any vote-counting software used in a Florida election be written in higher-level computer languages, because such languages are easier to analyze for errors or fraud.

d) Encourage the use in Florida elections of public domain software certified by an organization accredited by the National Institute of Standards and Technology. To further that end, the State of Florida, in a consortium with other states, should pursue the possibility of creating an organization of experts to certify the software. The consortium could then be certified by the National Institute.

e) Strongly encourage the use of dedicated computer equipment by the Supervisors of Elections.

(Legislation to accomplish many of these recommendations is included in the Appendices.)

Legal Issues Associated with Optical Storage

Based on the findings concerning the optical storage of documents, the following conclusions are drawn:

- Current law, s. 15.16, F.S., which expressly authorizes the admission of certain records of the Department of State into evidence, does not expressly authorize optically stored documents.

Therefore, it is recommended that:

14) Section 15.16, F.S., be amended to specifically authorize the Department of State to store documents through the use of optical

images and that those records be admissible as evidence in court. (Legislation to accomplish this is included in the Appendices.)

- Except for special cases, current law is silent regarding the use of WORM optical imaging for general archival and evidentiary purposes. This poses problems for custodians who wish to take advantage of the new technology.

Therefore, it is recommended that:

15) The House and Senate Judiciary Committees consider whether a general law is needed to address the use of optically stored documents. Some options for consideration include:

1) Specifically authorizing the admission into evidence of WORM optical images but excluding the admission of erasable ("write many, read many") images.

2) Authorizing the admission into evidence of both erasable and non-erasable optically stored records.

3) Specifically addressing whether paper originals of optically stored documents can be destroyed, and if so, after what period of time.

4) Specifically barring the admission of optically stored records into evidence.

It is further recommended that:

16) The Division of Library and Information Services, Department of State, promulgate rules for state and local agencies regarding the use of optical disk technology.

Dissemination of Public Information

Based on the findings regarding the dissemination of public information, the following conclusions are drawn:

- Florida has no coherent state policy concerning information dissemination by state agencies.

Therefore it is recommended that:

17) The Information Resource Commission address this issue in future State Strategic Plans for Information Resources Management and that agencies be required to include a policy statement on how they disseminate information to the public in their future Strategic Information Resources Management Plans.

- Libraries have historically been instrumental in disseminating information in printed form, and they could likewise be a focal point for the electronic dissemination of information.

Therefore it is recommended that:

18) The Division of Library and Information Services, Department of State, establish an on-line bibliography of public documents and archived documents.

Computer Software Issues

Based on the findings regarding computer software issues, the following conclusions are drawn:

- Some public agencies are copyrighting and selling their software in apparent violation of Chapter 119, F.S., the Public Records

Law. This practice is understandable given the short-term benefits to agencies and jurisdictions of collecting revenue in a time of fiscal constraint. However, when viewed with the long-term perspective of the public's interest, this practice is a threat to the public's ability to know about its government.

- Existing statutes, case law, and attorney general opinions indicate that, except for specific exemptions for certain types of software, most agency-produced software is subject to the inspection and copying provisions of Chapter 119, F.S.

Therefore, it is recommended that:

19) The existing law with respect to the inspection and duplication of public records be more stringently enforced by the State Attorneys.

It is further recommended that:

20) The Information Resource Commission, in conjunction with the Department of State and subject to available resources, study the feasibility of establishing a state clearinghouse for software exchange which would serve state and local governments.

- Proprietary software vendors may be reluctant to do business in Florida if contracts do not protect their copyright.

Therefore, it is recommended that:

21) The Division of Purchasing, Department of General Services, examine the existing contract language, specifically Rider 401.14, regarding Protection and Security of Licensed Program Materials, to determine if the standard contract language

concerning the protection of copyrights is sufficient in light of the California court case, BV Engineering v. University of California, Los Angeles, 858 F.2d 1394 (9th Cir. 1988). If it is not sufficient, the Division should revise the language to protect the vendors' copyrights.

Computer Matching

Based on the findings regarding computer matching, the following conclusions are drawn:

- The increased use of computer matching by federal and state agencies raises privacy and other concerns, since few administrative controls, procedures, or guidelines are in place, and currently there is no oversight of computer matching in Florida agencies.
- It is too early to determine whether the federal computer matching legislation, passed in October 1988, will provide the necessary controls for most matching activities conducted in state agencies or if additional state legislation is required to regulate those matching activities not covered under the federal law.

Therefore, it is recommended that:

22) The Joint Committee on Information Technology Resources monitor the implementation of the new federal law and the development of the President's Office of Management and Budget guidelines to determine whether state legislation on computer matching is needed.

Fair Information Practices

Based on the findings regarding fair information practices, the following conclusions are drawn:

- Large amounts of personally identifiable information are stored in state agency computers, and in many cases Florida does not provide statutory protections to assure the accuracy of such information.

Therefore, it is recommended that:

23) A Fair Information Practices Act be implemented in Florida. Such an act should apply only to state agencies and should exempt from its scope various types of information which have proven difficult for other states, such as information on prisoners. (Legislation to accomplish this is included in the Appendices.)

Technological Impacts on Privacy

Based on the findings regarding technological impacts on privacy, the following conclusions are drawn:

- Technological advances have improved government record keeping, detection and prevention of fraud, waste, and abuse, and law enforcement investigations. At the same time, opportunities for inappropriate, unauthorized, or illegal access to and use of personal information have expanded and threaten the privacy of individuals.
- Information law and government policy must respond to the current environment of changing cultural and social circumstances and rapidly developing technologies.

Therefore, it is recommended that:

24) The House and Senate Governmental Operations Committees consider legislation to allow individuals to request that their names and addresses contained in public records as defined in Chapter 119, Florida Statutes, not be released for commercial solicitation purposes.

25) The House and Senate Governmental Operations Committees consider legislation to create a statutory distinction between public records containing personally identifiable information and other public records, and to provide appropriate standards and restrictions for the handling and dissemination of such records.

Records Management and Archives

Based on the findings regarding archival and records management concerns, the following conclusions are drawn:

- The increased use of information technology to create, store, access, and disseminate information has not resulted in increased attention to the preservation of the public record or the increased complexity of records management in an information age.
- There is no evidence that the applications and systems being developed by agencies and local governments are explicity considering archival and dissemination issues, as was recommended in the Joint Committee's 1985 Report, Remote Computer Access to Public Records.

Therefore, it is recommended that:

26) State agencies be required to include records management and archival issues in their Strategic Information Resources

Management Plans and that the Information Resource Commission include these issues in their planning requirements.

27) Criteria be developed by the Information Resource Commission, with the participation of Division of Library and Information Services, Department of State, and the Information Resources Management Advisory Council, to assure that all new applications adequately address the archival and records management issues.

- o New technologies, including optical storage, electronic data interchange, and electronic mail, pose significant challenges to the state's archival and records management programs. The impact of state and local governments' adoption of these technologies on the public record is not clear.
- o There are no accepted national standards governing this new technology and the issues which concern public sector organizations are different from those of private sector organizations.

Therefore, it is recommended that:

28) The Joint Committee on Information Technology Resources monitor state agencies' use of optical storage, electronic data interchange, electronic mail, and other new technologies to determine if statutorily established archival and records management responsibilities require modification.

29) The Department of State and the Information Resource Commission participate in the standards setting processes of national organizations, such as the American Bar Association and the National Institute of Standards and Technology.

I. INTRODUCTION

Purpose

The state's information policy consists of many laws and rules governing how state and local governments collect, use, store, and disseminate information. State and local governments in Florida are increasingly adopting information technology as a way to improve the effectiveness and efficiency of their operations and their record keeping. The Committee's 1988 survey of state and local government record custodians indicates that over half of all public records in Florida are computerized. As more public records are automated, the applicable laws governing them, which were written when most records were paper documents, require review. The laws must reflect the impacts and changes brought about by technology. As a result of automation, common assumptions about government's role are being questioned and the traditional ways in which government performs its mission are changing. The purpose of this report is to examine the major issues arising from the impact of information technology on government information creation, storage, processing, and record keeping, and to make recommendations on the state's information policy in response to those impacts.

Methodology

The methodology for this report consists of three major information gathering efforts. First, a literature search was conducted and a References section is included at the end of the report. Second, several mailed surveys were conducted. One survey

was mailed to state and local record custodians in August 1988. This survey was a follow-up to one conducted by the Committee in 1984. It requested information on public records practices and solicited comments on problems experienced. A copy of the survey instrument is included in the Appendices. The 26-item survey was sent to 559 individuals and 302 responded, for an excellent response rate of 54%. The largest number of respondents were state agency information resource managers, followed by court clerks and sheriffs. Another survey was mailed to the ten states which currently have Fair Information Practices Laws. The 18-item questionnaire solicited their comments on how the law has been implemented in their jurisdictions. A copy of this questionnaire is included in the Appendices. The other mailed survey was sent to all Florida state agencies to determine the extent of their current computer matching activities. A copy of that 13-item survey is also included in the Appendices.

The third part of the information gathering process consisted of three public hearings held in Tallahassee, Ft. Lauderdale, and Orlando during January 1989. Testimony from invited speakers as well as the general public was received. Agendas from the three hearings are included in the Appendices. The hearings focused on the major issues previously identified by staff research. Those issues are the substance of this report.

Organization of Report

This report is organized into four major sections, beginning with this introductory section. Section II is a background chapter on Florida's Public Records Law, which is the centerpiece of the state's

information policy. Other laws addressing information policy are also highlighted in the background chapter. Section III of the report is organized according to the nine major issues identified by staff research. Each issue is a separate chapter in Section III of the report.

Following the issues chapters are the Conclusions and Recommendations, Section IV. A list of References and the Appendices follow Section IV. The Appendices include draft legislation to implement certain recommendations, copies of the survey instruments with responses, lists of the individuals who testified at the Committee's public hearings, and copies of key legal opinions pertaining to the computer software issue.

The public hearings were recorded and the tapes are on file in the Committee offices, as are the written remarks and other documents presented by the speakers.

II. BACKGROUND

The state's information policy is established in numerous statutes and administrative rules. A review of the Florida Statutes index reveals that there are over 120 laws which require a report to the Governor, and more than 200 laws which require a report to the Legislature. These laws reflect a state policy which encourages open communications and review of government activities. Public information on these programs is readily available in printed report form.

Over 300 laws deal with various aspects of government records and their management. For example, s. 28.24, F.S., establishes the fees to be paid for copies of records maintained by the Clerks of the Courts. Another law which the Joint Committee was instrumental in drafting in 1983 and in substantially amending in 1987, is the Information Resources Management Act, ss. 282.303-.314, F.S. This law requires that a statewide strategic plan for information resources management be prepared by the Information Resource Commission. It also requires agency strategic plans, operating plans and performance reports on each agency's information resource management activities. The law defines information resources management as,

> . . . the planning, budgeting, organizing, directing, training, and control associated with government information. The term encompasses both information itself and the related resources associated with its use.

The centerpiece of the state's information policy, however, is the Public Records Law, Chapter 119, Florida Statutes. Because of its importance in understanding the state's information policy, a brief history of the law and case law arising from it is provided.

Brief History of Public Records Law

An informed citizenry is fundamental to democracy. Open records laws enable individuals to inform themselves about the activities of the government and its officers. Madison recognized the importance of public records in a discussion of the implications of the First Amendment: "...the right of freely examining public characters and measures, and of free communication thereon, is the only effectual guardian of every other right..."[1] Judge Cooley, in his treatise on constitutional history, states that the First Amendment sanction was accorded not only to dissemination, but also to acquisition of information.[2]

A common law right providing limited access to public records was an early development of American legal theory. Under the common law, only a limited class of persons was allowed the right of inspection, because a legally recognized "interest" had to be demonstrated.[3] American courts have generally used a broad definition of "interest"; that of a public interest.[4] The common law rights evolved into public

---

[1]Quoting from The Writings of James Madison, 398 (1806). Reprinted in Access to Official Information: A Neglected Constitutional Right, 27 Ind. L. J. 209, 212 (1950).

[2]Thomas M. Cooley, Constitutional Limitations, 885, 886, 8th ed. 1927.

[3]Project: Government Information and the Rights of Citizens, 73 Mich. L. Rev. 971, 1178 (1975) [hereinafter cited as Project]. See e.g., Nolan v. McCoy, 77 R.I. 96, 103, 73 A.2d 693, 697 (1950).

[4]Id. at 71179, see e.g., Clement v. Graham, 78 Vt. 290, 315-316, 63 A. 146, 153-154, (1806); Moore v. Board of Chosen Freeholders, 76 N.J. Super. 396, 184 A.2d 748 (App Div.), modified on other grounds, 39 N.J. 2d 26, 186 A.2d 676 (1962); Nowack v. Auditor General, 243 Michigan 200, 219 N.W. 749 (1928).

records acts, enacted on both the state and federal levels, providing statutory guarantees of access to records.

Florida, in 1909, enacted one of the first public records laws in the nation. It stated, "all state, county, and municipal records shall at all times be open for a personal inspection of any citizen of Florida."[5] This statute was used as a model in a campaign for nationwide enactment of public records laws by the journalism organization, Sigma Delta Chi.[6] Public records were defined by an early Florida Supreme Court opinion as a "written memorial made by a public officer...[I]t is one required by law to be kept, or necessary to be kept in the discharge of duty imposed by law, or directed by law to serve as a memorial and evidence of something written, said or done."[7]

The federal government, in 1970, passed the Freedom of Information Act.[8] It provides that all government agency records be made available for public inspection unless expressly exempted by statute. A number of exemptions, including one for trade secrets, are provided for in the law.

---

[5]Ch. 5942, Laws of Fla. (1909).

[6]Freedom of Information Center, Access Laws: Defeats 2 (1962), noted in 33 U. of Fla. L. Rev. 313, 328 (1981).

[7]Amos v. Gunn, 84 Fla. 284, 343, 94 So. 615, 634 (Fla. 1922).

[8]5 U.S.C. 8552 (1970).

General Principles of Access in Florida

In broadening its application of the concept of open records, Florida, in 1967, amended its public records statute (Chapter 119) to read: "Every person having custody of public records shall permit them to be inspected and examined...by any person." The present revision of the state's policy was adopted in 1975 and reads: "It is the policy of this state that all state, county, and municipal records shall at all times be open for a personal inspection by any person."

Custodians or their designees are to supervise inspection. Attorney General Opinion 075-50, February 27, 1975, holds that a custodian may not charge a fee for the mere inspection of public documents The opinion states further that, "[s]imply stated, providing access to public records is a statutory duty imposed by the Legislature upon all record custodians and should not be generally considered a profit-making or revenue-generating operation."

Access to public records is controlled by five factors: the definition of public records, the number and substance of exemptions, the content and format of access, cost of access, and procedures for enforcement and sanctions for violations.[9] These are discussed below.

Definitions of Public Records

Florida's statute has broadened the common law definition of public records. Chapter 119, Florida Statutes, currently defines "public records" to encompass:

---

[9]H. Cross, The People's Right to Know, 6-7, 42-45 (1953), noted in 33 U. of Fla. L. Rev. 313, 329 (1981).

> ...all documents, papers, letters, maps, books, tapes, photographs, films, sound recordings or other material, regardless of physical form or characteristics, made or received pursuant to law or ordinance or in connection with the transaction of official business by any agency.

The Florida Supreme Court has construed this definition of public records to include "any material prepared in connection with official agency business which is intended to perpetuate, communicate, or formalize knowledge of some type."[10] Thus, even though a document is not in final form or does not represent the agency's ultimate product (such items as inter-office memoranda, for example), it is considered a public record. Materials which are not public records are those prepared as drafts or notes which "constitute mere precursors of governmental 'records' and are not, in themselves, intended as final evidence of the knowledge to be recorded."[11] Further, public records were held in Seigle v. Barry to include all information in a computer (which is as much a public record as the written page in a book), not merely that which a particular program accesses.[12] In the same case, the court stated:

> It is impossible to lay down a definition of general application that identifies all items subject to disclosure under the act. Consequently, the classification of items which fall midway on the spectrum of clearly public records on the one end and clearly not public records on the other will have to be determined on a case-by-case basis.

---

[10]Shevin v. Byron, Harless, Schaffer, Reid and Associates, Inc., 379 So.2d 633, 640 (Fla. 1980), noted in Florida Open Government Laws Manual at 37.

[11]Id. at 38.

[12]422 So.2d 63, 65 (Fla. 4th DCA 1982), pet. for rev. den'd, 431 So.2d 988 (Fla. 1983).

Exemptions

Under common law, exemptions were granted for those records which were private, secret, or confidential and those which, though public in the legal sense, were excluded from inspection based on public policy.[13] The courts used a balancing test weighing the importance of public access against the harm that might result from disclosure.[14] Florida courts provided exemptions to the Public Records Law well into the 1970's.

However, in 1979 the Supreme Court in Wait v. Florida Power and Light Co., adopted the view that only statutory exemptions are allowed to the Public Records Law.[15] Specific exemptions are stated in Chapter 119, though numerous others are contained in other chapters. The Florida Open Government Laws Manual identifies over 200 specific exemptions. Unless an exemption is specified, a record is presumed to fall under the Public Records Law. If, however, a public record has exempted information, the record keeper must delete that information from the document before allowing inspection. In the absence of a specific statutory exemption, even copyrighted material is subject to the Public Records Law for purposes of examination and inspection.[16]

---

[13] Project, supra note 3, at 1170.

[14] Id., at 1170-71, noted in 33 U. of Fla. L. Rev. 313, 330 (1981).

[15] 372 So.2d 420 (Fla. 1979).

[16] 1982 Op. Att'y Gen. Fla. 082-63 (September 1982), where the Attorney General stated the agency should not reproduce or distribute copies since that would violate the pre-emptive federal law on copyright.

There are two areas of non-statutory limitations on inspection. The first is the judiciary's right to control access to its own records. This is "because of the doctrine of separation of powers and because the Constitution vests in the Supreme Court the power to adopt rules for the practice and procedure in all courts."[17] The second area is legislative records concerning constitutionally confidential functions. While there are no cases on point, an Attorney General opinion holds that legislative records are subject to Chapter 119 if they are made or received in connection with official business and if there is not a House or Senate rule to the contrary.[18] The one exception to this is contained in s. 15.07, F.S., which states that ". . .the journal of the executive session of the Senate shall be kept free from inspection or disclosure except upon the order of the Senate itself or some court of competent jurisdiction."

In 1984, the Legislature enacted s. 119.14, F.S., otherwise known as the Open Government Sunset Review Act. This law requires periodic legislative review of all the exemptions to the Public Records Law and the Open Meetings Law. The Law provides three criteria for review of the exemptions and states that the exemptions shall be maintained only if one of those criteria are met. They are, as cited in the law,

---

[17] Supra, note 9 at 58-59. See The Florida Bar in re. Advisory Opinion concerning the applicability of Ch. 119, F.S., 398 So.2d 446 (Fla. 1981), in which the Florida Supreme Court concluded that the investigative files of the State Bar as the official area of the Supreme Court are subject to the control and direction of the court and not to the other branches of government and thus Ch. 119 does not apply to such records.

[18] 1975 Op. Att'y Gen. Fla. 075-282 (November 18, 1975).

(a) The exempted record or meeting is of a sensitive, personal nature concerning individuals;

(b) The exemption is necessary for the effective and efficient administration of a governmental program; or

(c) The exemption affects confidential information concerning an entity.

If exemptions are reenacted, they are subject to the same review in 10 years.

Content and Format of Access

Florida does not require a person desiring access to demonstrate a "special interest" to inspect a public record. Indeed, Florida is similar to most states in making the right of inspection available to any person, regardless of interest, purpose, or use.[19] The statute is silent, however, about the custodian's obligation to provide the public record in a specific format, such as a paper copy or a magnetic tape. Chapter 119 currently does not distinguish between a paper document which can be inspected or copied manually or mechanically, and an electronic record which can only be perceived if it is displayed on a terminal display screen, transformed into paper output, or recorded on magnetic media for "translation" at a later time.

---

[19] See, Florida Open Government Laws Manual at 47, 48. Cf. State ex rel. Davis v. McMillan, 49 Fla. 243, 38 So. 666 (Fla. 1905) (holding that abstract companies may copy public documents from the clerk's office for their own use and sell such copies to the public for profit).

This has resulted in conflicts between custodians and requestors over the content and format of access. Many record custodians have maintained that the provision of the records in any format, and in their customary manner, satisfies Chapter 119. Paper output, for example, may be provided rather than a magnetic tape. Requests for records have been received for all of the data stored in computers, even when there were no programs to access the data, or for specific arrangements of the data, or for additional processing of the data to create a new public record.

In Seigle v. Barry,[20] the court stated that record custodians do not have to provide access to computerized records in the particular formats requested by the user. Nor must the custodian provide new software (computer programs) to reorder the data or accept programs written by the requestor to reorder the data. Instead, the court held that the use of programs currently used by officials for maintaining the computerized records is all that custodians are required to provide the requestor.

Chapter 119, F.S., gives the Division of Library and Information Services of the Department of State the responsibility and authority to examine the condition of public records and provide advice and assistance to public officials about the preservation of such records. Microfilming records is specifically identified as a form of assistance. This transformation of documents into microfilm copies, a change in format, has not created legal conflicts, due to the

---

[20] Id. at 30.

simplicity of retrieval and the commonly understood principles of photography.

The Cost of Access

Access to public records includes the visual inspection and copying of records. In Winter v. Plaza Del Sol, Inc.,[21] the appellate court stated that the right to inspect public records carries with it the right to make copies because the right to inspect would in many cases be valueless without the right to make copies. A definition of "copy" is not provided in Chapter 119, F.S. However, most tangible forms, including photocopies, computer printouts, microfiche, and computer tapes, are generally considered "copies."

Although fees can be charged for the cost of the copies, in most cases these charges include only the actual cost of duplication. An informal opinion by the Attorney General dated June 28, 1978, advised that, unless otherwise provided for by law, the custodian of public records should charge no more than the actual cost of duplication for furnishing copies. (Emphasis added.) It was concluded therein that the actual cost of duplication does not include incidental expenses such as utilities, personnel, and other office expenses. Also, the Attorney General, in an informal opinion issued June 15, 1979, concluded that a person bringing his own copying machine should be permitted to plug into the agency's electrical supply.

---

[21] 353 So.2d 598 (Fla. 4th DCA 1977).

In a related Opinion, 082-23, April 9, 1982, the Attorney General opined that when a member of the public uses his own photographic equipment to make his own copy, the clerk is not entitled to the fees prescribed in s. 28.24, F.S., which pertains to service charges by the Clerk of the Circuit Court. Instead, the custodian is only entitled to the supervisory service charge provided for in that section.

Chapter 84-298, Laws of Florida, amended s. 119.07, F.S., and provides that the actual cost of duplication does not include the labor or overhead costs. However, it also states that a special service charge is allowable if the nature or volume of the records to be inspected or copied requires extensive personnel assistance. Chapter 85-86, Laws of Florida, also amending s. 119.07, F.S., provides further that a special service charge is allowable if "...the nature or volume of public records requested to be inspected, examined, or copied...is such as to require extensive use of information technology resources or extensive clerical or supervisory assistance, or both...." The special charge must be reasonable and based on the actual costs incurred by the agency. This language was added in response to some record custodians' complaints that requests for copies of entire computerized databases were frequent and required substantial computer resources. This law also providesd authority for custodians to provide remote electronic access to the public records, and to charge a fee for this type of access. The law was passed subsequent to the Joint Committee on Information Technology Resources' 1985 report and recommendations on the subject. Previously, Attorney General Opinion 076-34 stated that search fees allowed by some

sections of the statutes did not extend to searches done via computer terminal by a person seeking access to records.

Enforcement and Sanctions

When denied access to public records, individuals may institute civil actions to compel compliance. These actions are entitled to an immediate hearing and take priority over other pending cases. Whenever the court orders the records open for inspection, the agency must comply within 48 hours, unless the issuing court provides otherwise, or an appellate court intervenes within 48 hours staying the order. If the court determines the agency "...unlawfully refused to permit a public record to be inspected, examined, or copied, the court shall assess and award against the agency responsible, the reasonable costs of enforcement including reasonable attorney's fees."[22]

Sanctions for violations of the Public Records Law are provided for both exposing exempted records and willfully and knowingly violating any of the provisions of Chapter 119, Florida Statutes. If exempted records are exposed, the official violating the provisions for exemption will be subject to removal or impeachment and shall be guilty of a first degree misdemeanor punishable by a definite term of imprisonment not exceeding one year. The sanction for a person's willful and knowing violation of any provision of the act is also a first degree misdemeanor.

---

[22]Ch. 84-298, § 7, Laws of Fla.

III. FINDINGS

CHAPTER 1 - DEFINING REASONABLE ACCESS

Background

In Wait v. Florida Power & Light, the Supreme Court stated that "reasonable times" and "reasonable conditions" in the Public Records Law refer

> . . . not to conditions which must be fulfilled before review is permitted, but to reasonable regulations that would permit the custodian of the records to protect them from alteration, damage, or destruction and also to ensure that the person reviewing the records is not subjected to physical constraints designed to preclude review.[23]

In another case, Myakka Valley Ranches Imp. Assoc., Inc. v. City of Sarasota, a circuit court ruled that the city must maintain within the city limits all non-exempt public records so that they are easily accessible.[24]

Discussion

Increasingly, government information is stored electronically, and database management software is used to sort, manipulate and retrieve data as needed. The Committee's survey of public record custodians in Florida indicates that over half (57%) of them have computerized the majority of their records. More local government record custodians (61%) report that a majority of their records are

---

[23]Wait v. Florida Power & Light Co., 372 So.2d 420 (Fla. 1979)

[24]Myakka Valley Ranches Imp. Assoc., Inc. v. City of Sarasota, Case No. 85-1248 CA-01 (Cir. Ct., Sarasota Co., Fla. May 22, 1985)

automated than do state government record custodians (48%). There is also a significant increase in the number of record custodians who report at least some automation of records. Ninety percent of the custodians reported some automation in 1988, compared to 75% in 1984. Exhibit 1-1 shows the reported increase in automation by type of record custodian.

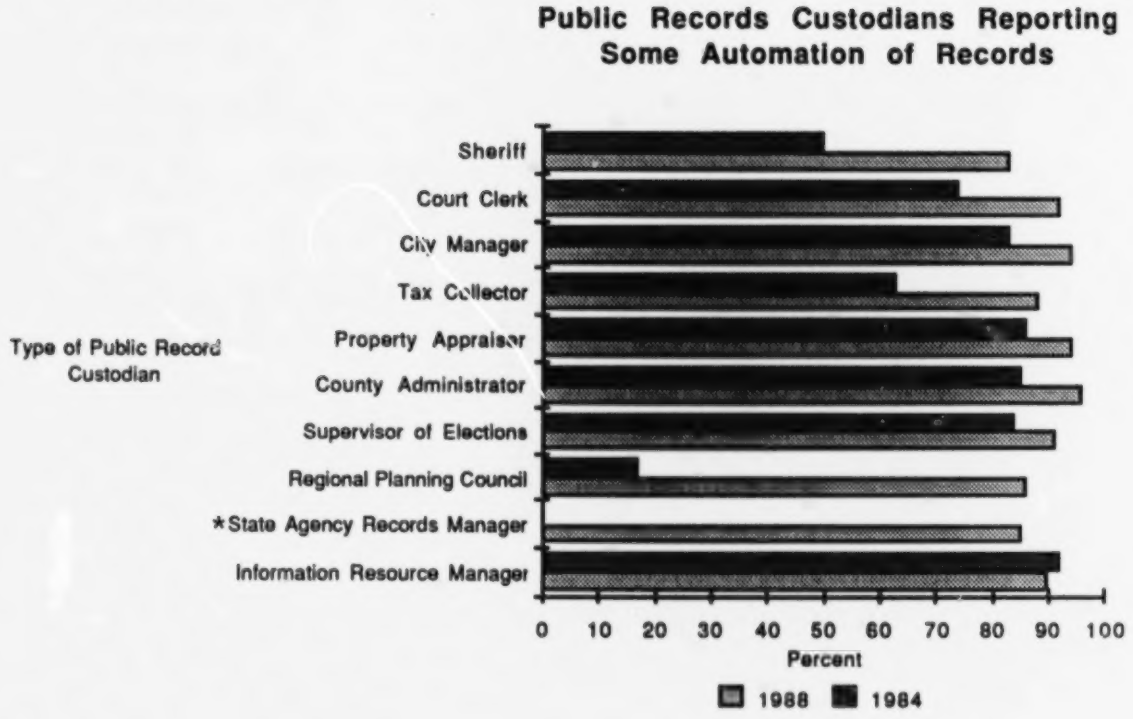
The automation of records and the use of sophisticated database management software have created an "information explosion." More than half (53%) of the agencies with automated records have installed a database management software system, although such systems are more prevalent in state agencies (79%) than in local government agencies (42%). There are now infinite possibilities for creating new public record information from information that already exists in the computer, since such existing information can easily be transported through networks, merged with other data, sorted and manipulated in many ways. The U.S. Congress' Office of Technology Assessment describes this as "the seamless web" of information.[25]

With manual record-keeping systems, the ease with which one can access records depends to some extent upon the filing system of the individual record custodian. Providing access to manual records generally requires assistance from personnel in the custodian's office. Once records are automated there are many ways to provide

---

[25]United States Congress Office of Technology Assessment, Informing the Nation: Federal Information Dissemination in an Electronic Age, OTA-CIT-396 (Washington, D.C.: U.S. Government Printing Office, October 1988) p. 8.

EXHIBIT 1-1



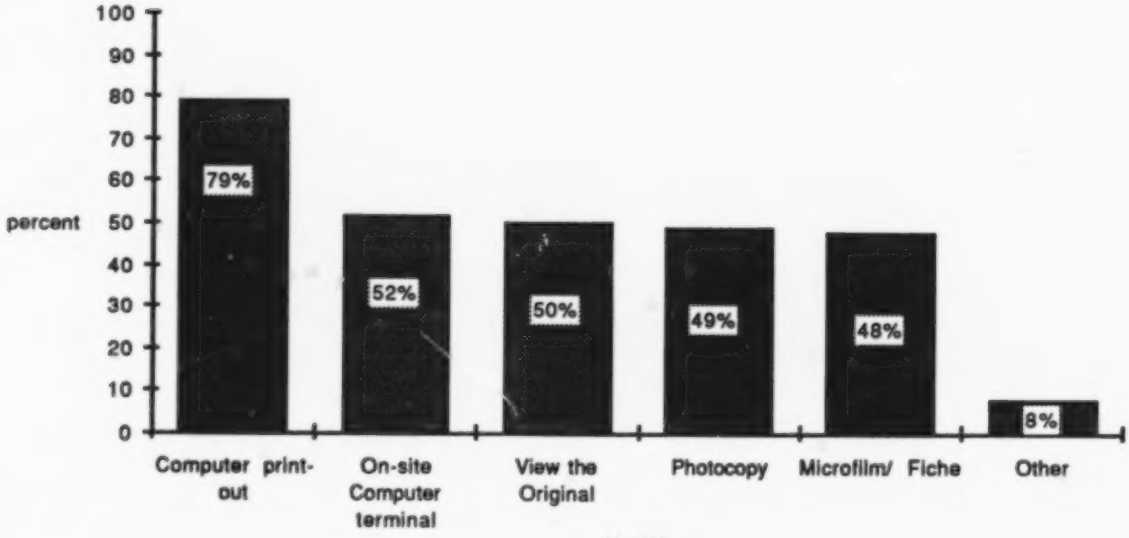
* State agency records managers were not surveyed in 1984.

access to them. Exhibit 1-2, based on the survey data, shows the multiple ways in which record custodians with automated records provide for their inspection. (Respondents could choose more than one response.) The most frequent (79%) method for inspecting automated public records in Florida is by providing computer print-outs. Over half (52%) of those with some automation provide inspection of records via a computer terminal located on-site, although much more frequently at the local government level (59%) compared to the state government (35%). Half of the custodians with automation allow for inspection of the original or by photocopy (50% and 49% respectively), and slightly less (48%) provide microfilm/fiche readers. The use of microfilm/fiche is much more common at local government agencies (59%) than at state agencies (21%). Eighteen percent stated they provide for remote electronic access by the public to their records. However, this figure is inflated due to erroneous inclusion of inter and intra-departmental networks by some respondents, as indicated in their remarks.

Only a small percentage (12%) of the record custodians with automated records stated that they were experiencing problems meeting requests for computer access to public records. Local government record custodians more often report problems (14%) than do state agency record custodians (7%). Those who are having problems cited such things as: too many requests from the private sector for mailing lists; too many requests for information and not enough staff resources to adequately meet the need; security problems related to keeping confidential information from public view; and inability to satisfy requests when particular formats or media are desired. One

EXHIBIT 1-2

Methods By Which Public Record Custodians Provide for Inspection of Automated Records



N=267

supervisor of elections wrote that "Candidates are requesting the Elections Office to be their software and mail order company."[26]

The vast array of information possibilities can create problems for record custodians in determining what is "reasonable access." For example, if records are maintained in an electronic format and database management software is available, should the public have the right to demand access in a certain manner? Although in Seigle v. Barry, the appellate court stated that custodians did not have to provide records in a particular format or devise new programs to reorder the data, the court did state that access to computerized records must be provided through programs used by the custodians.[27] Therefore, must public access methods keep pace with those in use by government agencies? This is an equity issue for the general public, but has economic and security ramifications for record custodians. Should the public be given stacks of printouts if a more useful form of access is possible? A 1986 congressional report states: "An agency must expect to upgrade public access to and use of agency records as its own information capabilities are upgraded."[28]

Alan Westin, Professor of Public Law and Government at Columbia University, testified at the Committee's Ft. Lauderdale hearing. He

---

[26]Survey respondent # 843

[27]Seigle v. Barry, 422 So.2d 63 (4 D.C.A. Fla., 1982) pet. for rev. denied, 431 So.2d 988 (Fla. 1983)

[28]U.S. House Committee on Government Operations, Electronic Collection and Dissemination of Information by Federal Agencies: A Policy Overview, (Washington, D.C.: U.S. Government Printing Office, April 29, 1986). p. 18.

addressed the need to empower the citizens by providing easy access to government information. He cited as an example that the Environmental Protection Agency was mandated by Congress to create a right-to-know database on hazardous wastes that was user-friendly and easily accessible. Westin recommends that the Congress and state legislatures mandate more dissemination of information. Otherwise, we will become a nation divided between the information-rich, the haves, and the information-poor, the have nots.

Westin is also Chairman of the Reference Point Foundation, which is a recently created non-profit organization that is developing a national on-line database and communications system to serve the voluntary sector and private citizens. When built, it will provide access to numerous government databases at lower fees than those charged by commercial vendors.

The automation of public records also presents a paradox: it provides the capability to more easily sort through numerous records and manipulate them in useful ways, and yet at the same time it can create obstacles to their access. As more records are automated, the manner in which the systems are designed for access, as well as the public's general level of computer literacy, may significantly affect how easily automated records may be electronically accessed. If records are not easily electronically accessible, many of the records may remain "hidden" from the general public.

When records systems are initially automated, the designers rarely take into account future public access requirements. Instead, systems may only be designed to meet a specific agency function. This

can make future provision of public electronic access expensive and difficult.

As governments automate virtually all of their records and maintain data in electronic formats, it will become necessary to assure that "access" is a design requirement. Systems must not only meet the functional specifications of agency users, they must also be able to satisfy the access requirements of the public. There has been no explicit policy statement regarding the ease of access. Case law supports record custodians providing only the computer programs that are used by the agency to search databases to requestors. However, during the transition to a completely automated government, it will be necessary to provide access in many formats and to assure that the needs of both skilled computer users and those who do not use computers are met. The selection of a specific database management system and fourth generation query language may need to be based on ease of use by the public. It may also become necessary to provide "help" screens and user manuals to the public to assure that access is not only available, but meaningful.

Thus, as public records become automated the "reasonable conditions" for access are more difficult to discern and ensure. A custodian may be faced with a very technologically sophisticated public which demands access to the database management software so that it can extract the records in the manner it desires. On the other hand, the same record custodian may also be faced with a computer illiterate public which requires assistance from personnel to extract records desired and feels more comfortable with paper

documents. The demands on the record custodian to provide inspection and copying are more complicated in the electronic age.

Some government agencies are successfully providing remote electronic access to public records in response to certain private sector interests. The Department of State has a contract with CompuServe Inc., a private sector network service, to provide remote electronic access to the Division of Corporations' records. These records include document filings for all active and inactive corporations registered with the state and all Uniform Commercial Code documents filed with the state. The system is menu-driven with help available for every part of the system. The Department publishes a 120-page "User Help Document" which takes a user through each step in the system, explaining the various screens and menus available.[29]

The Department of Highway Safety and Motor Vehicles also provides remote electronic access to selected driver license and motor vehicle records through the use of CompuServe, Inc. A Bureau Chief from the Department testified at the Committee's Tallahassee public hearing that they currently have 518 subscribers. He also stated that they are investigating the feasibility of allowing access by other private network providers. The Department provides two types of remote access. Remote electronic access, via either leased or dial-up phone lines, is interactive and is available from 11 a.m. to 6 p.m. Monday through Friday. Remote job entry allows a user to send several requests for information to the computer which stores them for later

---

[29]Florida Department of State, Division of Corporations, Public Access User Help Document, (Tallahassee, Florida).

processing. After processing, the computer stores them for retrieval by the requestor. Remote job entry submission is available from 4 p.m. to 6 p.m., Monday through Friday. The computer processes the requests from 10 p.m. to 4 a.m., Monday through Friday and allows retrieval from 4 a.m. to 9 a.m., Monday through Friday.[30]

The Department of Commerce provides the public with remote electronic access to several of its databases either through dial-up access to databases residing at FSU's computer center or through dial-up access to the Department's own microcomputer network. Some of the databases which can be accessed include: the building compendium, which contains information on vacant industrial buildings in Florida; the county profile, which contains statistical data on individual counties in Florida; the import/export data base which the Department receives annually from the U.S. Department of Commerce Foreign Trade Division; and a tourism database which contains historical and current information on over sixty types of data on tourism in Florida. To access the Commerce databases which reside at the FSU computing center, one needs a compatible computer terminal or microcomputer, a modem, and a valid FSU computer account number and password. To access the Department's microcomputer network one needs an IBM compatible microcomputer, a compatible modem, and a copy of a particular software communications package (Carbon Copy Plus).[31]

---

[30]Florida Department of Highway Safety and Motor Vehicles, Providing Records to the Public: Policy Number 010, (Tallahassee, Florida, January 15, 1988) p. 7.

[31]Florida Department of Commerce, Florida Facts: Computer Data Bases, (Tallahassee, Florida, September 1987) pp. 1-4.

The Lee County Property Appraiser's Office allows the private sector to access its records in two ways. First, any individual who is a member of the local board of realtors can access the records through the board's computer. The Lee County Property Appraiser sells tapes of his records to the local Boards of Realtors. The Boards hire a software firm to re-format the data so that it is more useful. According to the Lee County Property Appraiser's testimony at the January 18, 1989 public hearing, there are currently over 200 subscribers to this service.

The second way to access the Lee County data is by dialing in directly through a leased terminal connected to the county mainframe. Private industry is paying for the hardware costs, in this instance. This second form of remote electronic access in Lee County is expected to be operational in 1989.

Section 119.085, F.S., governs the provision of remote electronic access to public records in Florida. It specifies two different conditions for determining the costing mechanism to be applied. If remote access is generally available to the public, then the fees charged are governed by the usual charges for copying records under s. 119.07, F.S. However, remote electronic access may also be established as a special form of access for certain users whereby the total costs of providing the access are recouped. This form of access requires a contract between the custodian and the user and is the form of access most often used, to date, by agencies providing remote electronic access to their records.

Other examples of successful remote electronic access to public records exist around the country. Utah has a system similar to

Florida's Division of Corporations: they provide remote electronic access to all corporate records and statewide UCC information through a service called "Data Share."[32] Montgomery County, Pennsylvania, has provided remote electronic access to certain records since 1981. The county provides public terminals on-site as well as dial-up access for remote users. The information available includes criminal justice case information, land records, tax records, deed records, and building permits.[33] Similarly, in San Diego, California, the city clerk has instituted a remote electronic access to public records system known as LEGIS, or Legislative Information System. This system is a collection of databases containing all of San Diego City's law, policies and legislative actions. The inclusion of other databases is planned for the future.[34] At the federal level, the Department of Agriculture in 1985 established a system for electronic dissemination of information to the public. It identified certain time-sensitive reports that were desired by many users other than individual farmers, such as farm organizations, trade associations, and the news services. It contracted with a private sector company to provide the computer time sharing service. The contract requires that the access be provided on an equal basis to all who pay for the automatic dial-out

---

[32]"Utah Data Share Online," Government Technology, January/February 1989, p.4.

[33]Letter from Robert MacNeel, Data Processing Director, Montgomery County, Pennsylvania, August 1, 1988.

[34]Charles G. Abdelnour, City Clerk, LEGIS: The Legislative Information System (San Diego, California: 1987)

feature, which relieves the users of the necessity to inquire interactively with the system.[35]

Current law in Florida provides that the record custodian may impose a special service charge for inspecting and copying records only if extensive use of personnel or extensive use of information technology resources are required. With automated records, there are unlimited possibilities for requests for data and the custodian must define what "extensive" means. That determination varies from one agency to another. For example, the Collier County Sheriff's office charges extra fees for each additional increment of personnel time required in excess of five minutes for the duplication of documents.[36] The Department of Highway Safety and Motor Vehicles charges an extra service charge whenever total personnel time on one request exceeds one hour.[37] In Seminole County, "extensive" means the "use of information technology resources in excess of 10 minutes or clerical or supervision assistance in excess of 20 minutes."[38] This underscores the survey finding that only 21% of the custodians have a formal charging system based on a cost collection/cost allocation model for determining costs to be charged for copies. State agencies

---

[35]Roxanne Williams, "Getting the Word Out" Government Data Systems, June/July 1985, pp.28-29.

[36]Sheriff Aubrey Rogers, Cost of Reproduction of Reports (Collier County, Florida: May 23, 1988).

[37]Florida Department of Highway Safety & Motor Vehicles, note 30, supra.

[38]Board of County Commissioners, Resolution No. 88-R-152 (Seminole County, Florida: May 10, 1988) p. 1.

are twice as likely to have such charging systems as are local agencies.

Almost half (49%) of the survey respondents with automated records report that they receive requests for copies of large portions of their computerized databases. Property appraisers and supervisors of elections are the record custodians most often receiving these types of requests. If custodians are faced with requests for daily updates to their entire database, is it "reasonable conditions" for access if the custodian limits copies of public records to a certain number per month or per year?

The automation of records and the increased networking of records systems have also created multiple record custodians for the same data. For example, in some counties one central data processing department may be responsible for maintaining the records for several different constitutional officers, such as the sheriff, tax collector, and the property appraiser. In such cases, the records are not maintained by the same individual who is responsible for collecting the original data. However, Chapter 119, F.S., does not make any distinction between a record "custodian" and a record "owner." In fact, s. 119.07(1)(a), F.S., states in part, "Every person who has custody of a public record shall permit the record to be inspected and examined...." (Emphasis added.) Attorney General Opinion 86-69, states "the fact that a particular record is also maintained by another agency does not relieve the custodian of either agency of the obligation to permit inspection or copying in the absence of an applicable statutory exemption."

As more records are automated and networked through communications with other systems, access becomes easier in some ways since there are numerous sources for the records. In effect, there can be multiple custodians providing "reasonable" access. This issue arose most recently in one Florida county when the sheriff was reluctant to release certain public records to the local press. The press then sought the records from the data processing director who maintained them. The director was unsure whether he was obligated to provide access to the records when the originator of the data, the sheriff, had denied access to them. This illustrates the survey finding that only 23% of the record custodians have written policies on access to computerized public records.

The increased automation and networking of public records creates new dilemmas for public records custodians in determining what is "reasonable" access in an electronic age. However, the choices that are made regarding how public access to electronic records is provided will largely determine the degree to which our public records are "open."

Summary

The courts have ruled that "reasonable times" and "reasonable conditions" under the public records law refer to rules which allow easy access to records by the public while also ensuring the protection of those records from damage or alteration. The majority of government information in Florida is stored electronically, and almost half of the systems utilize a database management software system to more easily sort, manipulate and retrieve data.

Once records are automated, there are numerous possibilities for providing access. This array of possibilities makes it more difficult to determine what is "reasonable access." As more public records are automated, the manner in which the systems are designed for access, as well as the public's general level of computer literacy, may significantly affect how easily automated records may be electronically accessed.

Innovative public records custodians in Florida and around the country have responded to the new opportunities offered by the technology and provide remote electronic access to public records. Current Florida law allows record custodians to charge a special service charge for the inspection and copying of records if it requires extensive use of personnel or extensive use of information technology resources. With automated records, there are unlimited possibilities for requests for data and the custodian must define what "extensive" means. Only 23% of the record custodians report that they have written policies on access to computerized public records.

CHAPTER 2 - SECURITY CONCERNS

Background

Recent news reports of a computer "virus" which temporarily crippled thousands of computer systems across the United States illustrate the particular vulnerabilities facing record custodians in an electronic age. Various Florida laws require record custodians to provide security for public records. Chapter 119, F.S., requires records to be kept in safe places. Chapter 282, F.S., requires each state agency to conduct a risk analysis of security threats to data and computer equipment and to provide a security program to alleviate or lessen the security risks. Chapter 228, F.S., authorizes the Division of Library and Information Services of the Department of State to establish and administer a records management program for both state and local governments.

Chapter 101, F.S., governs voting methods and procedures, and requires, among many other things, that the Department of State promulgate rules establishing minimum security guidelines for electronic and electromechanical voting systems. In the 1988 national election, it was estimated that over half of the total votes were counted electronically,[39] which makes the issue of computer security of these systems crucial to ensuring a fair and accurate election.

---

[39]Ronnie Dugger, "Annals of Democracy -- Counting Votes" New Yorker, November 7, 1988, p. 40.

Discussion

With paper records, the biggest security threats concern the physical integrity of the document itself, including security from fire, theft, mutilation, alteration or destruction. Typically, record custodians supervise the public inspection and copying of original paper records as a means of securing them, or they provide photocopies or microfilm copies for that purpose. However, the security threats are greater in automated record systems, particularly if the "original" only exists in its electronic form. Disgruntled employees may sabotage security systems and alter or destroy records. "Computer hackers" may break security codes and breach confidential information or destroy vital data or programs. Through computer fraud a person can embezzle money or change the outcome of an election. The impacts of unintentional and innocent security breaches such as errors or omissions, are also more problematic in electronic systems. In fact, recent data from the national studies show that employee errors and omissions are the major computer security problem, accounting for 65% of all data processing losses.[40]

Custodians of manual records systems have always dealt with both record-related security issues and access-related security issues. Record-related security concerns include assurance that the records are accurate and that confidential data is protected. Access-related security concerns include assurance that only authorized persons can

---

[40]Florida Information Resource Commission, Florida's IRM Quarterly Review, (Tallahassee, Florida: January 1989) Vol. 3, No. 1, p. 8.

access the system and that their access does not go beyond public record material. These security concerns have become more problematic with the advent of electronic records systems. In some ways, the more secure the automated system, the less accessible are the records. One of the respondents to the Committee's survey stated, "Systems and records must be secure, but not to the extent that innovation and imagination are stifled."[41]

Computer networking increases the exposure of those systems to security risks. It is an axiom that such systems are only as secure as their least secure element. The American Bar Association estimates that a billion dollars a year are stolen by "electronic cat burglars."[42] There are documented instances of dishonest employees raising their own salaries and dishonest students raising their grades through computer fraud.[43]

The demands for security and the demands for access often conflict, but such conflict is not necessary or inevitable. Historically, automation of public records systems did not include planning for public access and the means of addressing access-related security concerns were not designed into systems. Today, security concerns are often used to deny remote electronic access. When public access is built into the initial design of a records system, such access can be provided efficiently and without compromising security.

---

[41] Survey respondent # 179.

[42] Dugger, p. 44.

[43] Id.

Two Florida agencies provide good examples of how remote electronic access has been provided without weakening security. The remote access systems of the Department of State and the Department of Highway Safety and Motor Vehicles have multiple levels of security. First, all remote access comes through CompuServe Inc., a private sector network service, which initially checks for one's authorization to be on the system. The Department of Highway Safety and Motor Vehicles also requires a user to present a valid password and account number assigned to him by the Department. Second, once a user is authorized access, both of the departments' software application programs limit the user to inquiry access only; the user can view but not alter or erase data. The user is locked into that mode of operation.

The Department of Commerce's network security for its remote electronic access system is similar to Highway Safety's. User names and passwords pre-authorized by the department are required for any user. The system allows users three tries to log-on before being disconnected from the system. Once users establish access to the microcomputer network, they have "read" or inquiry access only: they cannot alter the information. Also, if users fail to access the network for more than 5 minutes, they are automatically disconnected or logged off from the system.

Security for remote electronic access can be provided in other ways. For example, an agency could establish a separate computer system dedicated to remote computer access which would have a duplicate set of its "live" system information. In this situation, remote users would never be able to enter the "live" data files, even

for viewing. Another network security method requires users to hang up after dialing in, so that the computer can call back, thereby ensuring that only authorized users gain access. In some instances, the cost of retrofitting security programs to allow public access may be greater than the benefits received by the efforts. The alternative is to provide other forms of access; however, incorporating remote access in the system's initial design will usually reduce the importance of the cost issue.

Section 282.318, F.S., which was originally proposed in a report of the Joint Committee, establishes the state's program for the security of data and information technology resources. The law requires each agency to appoint an individual to serve as the agency information security manager (ISM). Each agency must conduct a risk analysis to determine the agency's security vulnerabilities, develop a plan to alleviate those risks, and periodically perform an audit of the procedures established. Since the law was passed in 1984, none of the agencies have been granted additional funding to meet this requirement, thus handicapping their ability to ensure computer-related security. One survey respondent noted, "staffing of specialized security positions at each state data center is desperately needed to even approach compliance with state law and security standards and guidelines."[44]

This law also requires the Information Resource Commission (IRC) to establish statewide security standards and rules to insure

---

[44]Survey respondent # 179.

consistency in practice among the agencies. In 1987, the IRC received a special appropriation to assist with a disaster recovery planning project to benefit all agencies. The potential security risk posed to data centers by a disaster, such as a hurricane, fire or bomb which could destroy their processing capabilities, was cited as a major concern of the agency information security managers. The IRC contracted with the accounting firm of Ernst & Whinney for assistance in developing the disaster recovery plan. Their findings indicate that the state needs a disaster recovery facility to provide alternative processing capabilities for the state's critical data processing applications. Some of the critical applications identified in the study include the Law Enforcement Stolen Motor Vehicle Information System and the DHRS' Abuse Registry, Food Stamp, and AFDC systems. Legislation to implement a facilities management form of a "hot site" is included in the Appendices.

The election year of 1988 focused public attention on the security of computerized voting systems. Voters were justifiably concerned about whether their votes counted once, twice, or not at all. The software that tells the machine how to count the votes can be written so that the outcome of an election could be improperly affected, but the instructions in that software are generally kept confidential because of trade secret protections.

For example, a program could be written that would automatically transfer some votes for one candidate to another at a certain time, or that would automatically add votes to a particular candidate, or that would pre-determine the outcome by a certain percentage. And, according to some experts in the field, some of

these "Trojan horse" programs would be extremely difficult to detect.[45]

A detailed analysis of computer voting appeared in the November 1, 1988, issue of The New Yorker. It stated that errors and accidents in computerized elections have occurred across the country and have increased in recent years. In an election in Manatee County, Florida, a seventh of the county's precincts had to be recounted when soggy ballots warped and were mangled by the equipment. An apparent software "glitch" or error was responsible for an incident in Ft. Pierce when a machine would count the Democratic votes, but would not accept Republican ones.[46]

The article details other incidents of software problems. In one Montana city in 1968, the votes for Humphrey and Nixon were interchanged. Montana law now permits voters to demand paper ballots. In one Nebraska county the electronic vote count one year showed more people voting than were registered to vote.[47]

Ballot cards used in electronic voting systems are also subject to tampering. According to the New Yorker article, "election workers, if they are dishonest, can punch extra holes in ballots to invalidate votes that have been correctly cast or to cast votes themselves in races the voter has skipped."[48]

---

[45] Dugger, pp. 45, 100.

[46] Id. at 58.

[47] Id. at 57-58.

[48] Id at p. 40.

Electronic elections security experts disagree on the precise degree of risk involved in computerized voting machines. However, Neil Heighberger, Dean of the College of Social Sciences at Xavier University, has studied the subject and concluded that computerized punch-card voting causes "technological disenfranchisement."[49]

At the public hearings, the Joint Committee heard from many witnesses on computerized voting systems. The Director of the Division of Elections, Department of State, stated that 41 of 67 counties use electronic voting systems, and that she is concerned about the security of those systems. She also stated that her office is understaffed for its responsibilities to certify equipment as required by law. She added that with the assistance of a state Service Through Applied Research (STAR) grant, her office would develop new and improved procedures for recertifying existing systems.

The local Supervisors of Elections who testified at the hearings expressed more confidence in their electronic voting systems than did the Director of the Division of Elections. The supervisors detailed their elaborate procedures for ensuring an accurate and honest vote tally. Most suggested that they could do a better job and perform manual recounts of a percentage of the total votes if the time between the primaries and the general election were lengthened.

Public confidence in both the integrity and accuracy of computer voting systems is essential to the legitimacy of elections. Roy Saltman, a computer scientist with the National Institute of Standards

---

[49] Id.

and Technology, testified at one hearing that poor management and operating procedures pose a greater security threat to the elections process than does computer fraud. He suggested that manual recounts for a small percentage of votes be required to help restore public confidence in the system. Several other states, including California and Texas, have codified those approaches.

He also recommended eliminating pre-scored punch cards to reduce the possibility for miscounts due to "hanging chad" on the computer card. Hanging chad are the bits of material which remain on incompletely punched pre-scored ballot cards which should have been removed by the voter using the stylus but were not. This hanging chad prevents the computer from accurately counting votes. He recommended phasing out the use of the antiquated lever machines since they are difficult to maintain and provide no paper audit trail. He further recommended that elections supervisors have dedicated computer equipment, rather than sharing a system with others.

Summary

Various Florida statutes require record custodians to provide security for public records. With paper records, the biggest security threats concern the physical integrity of the document itself, but automated record systems create new security risks. Public records custodians face conflicting demands to provide easy access and yet retain a secure system.

When public records systems are first automated, there usually is not conscious planning for electronic access to those records by the general public. The networking of different computers increases the

exposure of the systems to security risks, since the system is only as secure as its least secure element.

Public record custodians frequently cite security concerns as reasons why they do not provide remote electronic access to the public records, but Florida agencies have successfully accomplished such access without compromising security.

A high priority security need for the state is the provision of a "hot-site" facility. Such a facility would provide data processing for critical applications in the event of a disaster.

Computerized voting systems, which have become the most common form of voting in Florida and elsewhere, also create security issues. The software responsible for counting the votes are generally not subject to public scrutiny since they are considered "trade secrets" by the firms which market them. There have been numerous incidents of error and accidents in computerized elections, both in Florida and around the country.

CHAPTER 3 - LEGAL ISSUES ASSOCIATED WITH OPTICAL STORAGE

Background

In 1949, the Florida Legislature created s. 92.36, F.S., which authorized the admission in a court of law of relevant records "kept by means of electronic data processing." The language did not indicate whether this statute applied exclusively to the government or the private sector. Thus, the assumption was that the statute applied to both. This statute was superseded in 1976 by the Florida Evidence Code, Ch. 90, F.S. The drafters of the Evidence Code believed that the express authorization of records stored in electronic data processing systems was unnecessary because such records would be admissible under the business records exception to the hearsay rule.[50] Hearsay evidence, defined as any assertion made out of court and offered to prove the truth of the matter asserted, is generally barred from admission in court. However, the Legislature created several exceptions to this general rule. The business records exception provides that records kept in the regular course of conducting business are admissible as evidence. The theory is that if a business relies on the accuracy of the record for conducting its affairs, the information must be reliable. Because of this assumption, the fact that the information won't be tested for veracity under the rigors of cross-examination is not as great a concern as it is in the classic hearsay case. Thus, if records are optically stored in the regular

---

[50]Personal interview with Professor Ehrhardt, Florida State University, College of Law, October 1988.

course of business, they may be admissible under the business records exception.

In 1967, s. 15.16, F. S. was created. This statute applies exclusively to the Department of State and authorizes the recording of records by means of electronic data processing and the admission into evidence of records stored by means of photography or micro-photography. Thus, it appears that the Department of State records which are optically stored are legally recorded but are not admissible in court, since they are not included in the definition of photography or microphotography. During the 1988 legislative session, SB 475 (companion to HB 618) passed the Senate but died in Messages. It would have provided, among other things, that optical images of records required to be filed with the department would have the same force and effect as the original records.

Discussion

Optical disk technology is one of several forms of electronic reproduction.[51] Two types of optical disks exist: erasable and non-erasable. Non-erasable optical disk technology is called WORM, which stands for "write once, read many." Information entered on a WORM disk can be viewed, but cannot be altered or erased. The information on such a disk is identical to the original information. Because the WORM optical disks are non-erasable, the risk of documents being altered by hackers, disgruntled employees, and embezzlers is

---

[51] Section 90.951(3), F.S.

significantly reduced. However, newer erasable optical disk technology creates a risk that users may tamper with documents.

Optical storage is a new technology. Courts are just beginning to be confronted with the legal issues that this technology raises. The significance of whether optical storage is an original or copy attaches when the optically stored document is sought to be introduced as evidence in court. Whether optically stored images are originals or copies may simply be a question under the Best Evidence Rule, i.e., whether the image is the best reliable, accurate evidence available under the circumstances. The Florida Evidence Code, s. 90.951(3), F.S., defines an "original" as:

> the writing or recording itself, or any counterpart intended to have the same effect by a person executing or issuing it. An 'original' of a photograph includes the negative or any print made from it. If data are stored in a computer or similar device, any printout or other output readable by sight and shown to reflect the data accurately is an 'original'.

It appears consistent with this definition that optically stored images be considered "originals." An example of an electronic image used as an original is found in s. 382.004, F.S., Microfilming and Destroying Records. This section authorizes HRS to reproduce vital records by "electronic means" and then to destroy the original paper documents and certify copies of vital records from the electronic image. It also provides that electronically produced certifications "shall have the same force and effect as the originals thereof, and shall be treated as originals for the purpose of their admissibility

in any court or case where the documents have been duly certified by the department."[52]

Another example is found in s. 92.295, F.S., created by Ch. 88-45, L.O.F., which provides that electronic copies of voter registration records are to be treated as original records. It also authorizes the destruction of original paper documents.

The Director of the Division of Corporations, Department of State testified at the Committee's January 9, 1989 public hearing that a Uniform Commercial Code optical disk prototype system will be operational in January, 1989 and will have an electronic certification system. The public may directly access the system through dial-up access. It is estimated that 80,000 U.C.C. inquiries are processed each day by the Division. Instead of archiving the paper documents to microfiche/film, the Division will archive to the optical disk system. The Division relies on s. 15.16, F.S., for its authority to archive in this manner. It also plans to dispose of the paper records as soon as they are no longer needed for fiscal information. Presently, the Division retains the paper copies for records archived on microfilm/fiche.

Although specific Florida Statutes reflect the national trend among state legislatures to accept electronically produced documents as originals, the Florida Department of State has not adopted rules on the use of this technology for records management. The Director of the Division of Library and Information Services testified at the

---

[52]Section 382.004, F.S.

Committee's Tallahassee hearing that the Division is recommending against the use of optical storage for permanent records until national standards are established. Nevertheless, the Division of Purchasing, Department of General Services has entered into a state contract for optical imaging systems, reflecting the demand for such systems by state agencies.

Other states, particularly Texas, have been struggling with this issue. Texas House Bill 163, which passed in July 1987, permitted the use of optical disks for storing real property records and some school records. The bill has not been implemented, however, because the Texas Attorney General, Jim Mattox, barred Texas county clerks and school districts from using optical disk storage systems until the American National Standards Institute (ANSI) adopts standards for archival permanence. A number of legislative flaws in the bill, as passed, have been communicated to the Texas Governor's Office:

1. Failure to require a permanent record - the bill does not require that a permanent backup copy be generated. Land records recorded on such a system would not be permanently protected.

2. Lack of system standardization - national or state wide standards for the technology have not been developed. Thus, it is not certain whether today's optical disks may be read by tomorrow's hardware.

3. Vulnerability to content alteration - the bill did not prohibit the use of "erasable" optical disk systems. The use of such

systems could jeopardize the integrity of Texas' Real Property Records and compromise property owners' rights.[53]

The federal trend appears to be acceptance of the legality of optical storage. For example, the United States Internal Revenue Service (IRS) is leaning toward accepting optical disk images as evidence in court. The IRS and the Justice department are "virtually certain" that the Uniform Photographic Copies of Business and Public Records as Evidence Act (28 US Code 1732) would permit destruction of original tax returns that were previously recorded on optical disks.[54] Optically stored images would be admissible under 28 US Code 1732 if the IRS could demonstrate that: 1) the contents on the disk could not be tampered with; 2) the complete tax return was copied; and, 3) image storage and retrieval was subject to suitable controls. These requirements are consistent with those established for demonstrating the legal acceptability of micrographic record images.[55]

In January 1988, the National Archives and Records Administration began developing government-wide standards for optical disk use. A key issue is maintaining data integrity. If adopted, these standards are expected to stimulate general federal agency use of optical disk systems. The National Archives' optical image storage system is

---

[53]Douglas P. Allen, "Optical Disk and the Law Texas Style," Inform, April, 1988, p. 44.

[54]"U.S. Government Agency Continues Efforts to Define Legal Acceptability of Optical Disk Records," EDPACS: The EDP Audit, Control and Security Newsletter, Vol. XV, No. 11, May 1988, p. 13.

[55]Id.

testing the conversion of 1.5 million documents to optical storage.[56] The National Archives and Records Administration (NARA) issued a bulletin stating that given the absence of standards ensuring the portability from one system to another, permanent records may not be stored on optical disk. This NARA bulletin will remain in effect until August 31, 1990. However, agencies may use optical disk systems for storing and retrieving permanent records while they remain in an agency's legal custody, provided no permanent records are destroyed after copying onto an optical disk without NARA's approval. This is similar to the advice given to agencies by Florida's Secretary of State.

The Veterans Administration (V.A.), St. Louis Regional Office, is testing a prototype optical disk system to process applications for educational benefits. The massive paper files provided the impetus for this project. The V.A. cites many advantages associated with optical disk storage: 1) more management control over the files; 2) files are easy to find; 3) files don't get lost; 4) more than one person can view the file at any given moment; 5) physical space is saved; 6) phone inquiries can be processed faster; and, 7) the system reports on the productivity and age of cases which minimizes delays in issuing benefits. However, the Veterans Administration is retaining the paper documents because their general counsel is not certain that

---

[56] Id.

documents stored on optical disk are legally admissible as evidence in court.[57]

The private sector is implementing optical disk technology to save time, money and space. Citicorp electronically transferred 50,000 hazard insurance policies, which corresponded to mortgage contracts, to Lomas Financial when Lomas purchased the mortgages. The exchange was treated as facsimile information which verified the existence of insurance coverage. It was not purported to be an original document. According to Tom H. Carter, Senior Vice President of Lomas Insurance Services, "If it were the mortgage or deed of trust, that would be different."[58] Carter did not comment on why he believed it would be different. However, one may surmise that the instruments' authenticity and negotiability would be foremost in such an evaluation.

Summary

There are two types of optical disk technologies: erasable and non-erasable. The non-erasable technology provides for increased data integrity because once recorded, the information may not be altered. Optical storage is a new technology, and the law is just beginning to grapple with the issues resulting from the use of the technology. Whether an optically stored image is an original record or a copy is a

---

[57]Mitch Betts, "Vets Say Optical Disk Will Kill Piles of Paper," Computerworld, September 5, 1988, p. 27.

[58]Alan J. Ryan, "Insurer Samples Optical Disk Transfer," Computerworld, October 3, 1988, p. 18.

significant issue, as is the admissibility of optically stored documents as evidence in court.

Section 15.16, F.S., authorizes the Department of State to record information by means of electronic data processing and admit into evidence information stored by photography or microphotography. Given the express authorization of admission into court of only certain records, it appears optically stored records are not admissible because they are not expressly mentioned. This follows the long-standing statutory rule of construction, expressio unius est exclusio alterius (the mention of one thing implies the exclusion of another).

The Florida legislative trend is to accept electronically produced documents as originals. Section 382.004, F.S., authorizes the Department of Health and Rehabilitative Services to electronically reproduce vital documents, destroy the paper originals and make certified copies from the electronic image. Chapter 88-45, Laws of Florida, authorizes an electronically generated reproduction of an original voter registration record to be treated as as original record. State and local government agencies may purchase optical imaging systems from a state contract for such commodities. However, no administrative rules exist for the use of such systems.

Other states, particularly Texas, have tried to resolve the questions raised by the use of this technology. Private sector and federal trends in the use of optical storage media indicate increasing acceptance of its evidentiary value. However, the National Archives and Records Administration has issued a rule which states that no

permanent records may be stored on optical disks until August 1990, when standards should be in place.

CHAPTER 4 - DISSEMINATION OF PUBLIC INFORMATION

Background

An informed citizenry is essential to democracy. Democratic governments have historically considered information distribution as an essential and non-controversial responsibility. Governments can help ensure an informed citizenry by providing easy access to public records and by actively disseminating information to the public. In Florida, Chapter 119, F.S., establishes the policy of open records, and Chapter 286, F.S., provides for open meetings. Chapter 257, F.S., provides for public libraries to serve as depositories of public documents. Additionally, many agencies are required to file annual reports with the Governor, Legislature, or both.

Discussion

State and local governments disseminate public information in many different ways. Written pamphlets, printed reports, and posters placed in public buildings are some of the more traditional ways of informing the public. Public libraries have also served as depositories of public documents. With the advent of radio and television, public service announcements became a new way of disseminating public information. The Florida Legislature has taken that one step further by underwriting the costs of a television program, "Today in the Legislature," which highlights the daily activities of the legislative session. This is a particularly effective way of disseminating information to citizens who cannot personally attend legislative meetings and sessions.

Information technology provides new ways to disseminate information. The use of computer terminals connected to public data centers provides for both on-site and remote electronic access to records. The State Library of Florida has a federal grant to help develop an on-line bibliographic database of all public documents. Once established, this information will be electronically disseminated to libraries throughout the state.

With the automation of public records, it is much easier for vast quantities of information to have "value added" by processing raw data in specified ways and by merging that data with other relevant data bases. Data is seen more often as an asset, and as something which is marketable. This has created a comparatively new private sector business for the repackaging and selling of public record information. The Office of Technology Assessment reports that, in 1986, there were 3,200 on-line database services available worldwide, and that the industry is growing at a rate of 15 to 18 percent a year.[59] Public agencies now find themselves, in some cases, competing with the private sector in disseminating information.

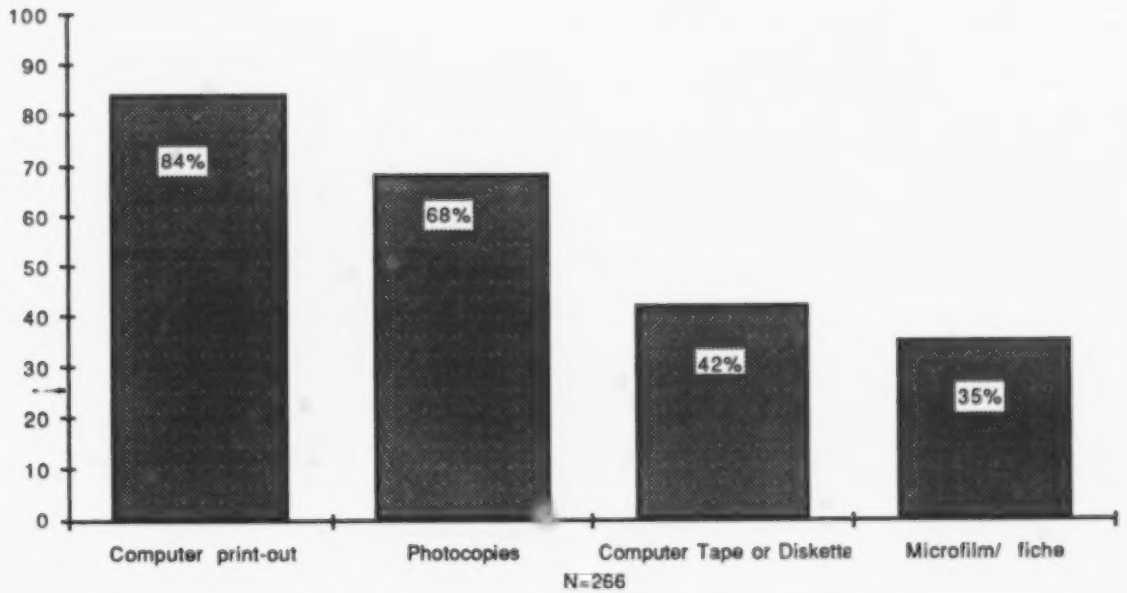
The Committee's survey of public record custodians indicates that copies of public records are provided in numerous ways, including electronic formats. Exhibit 4-1 shows that nearly half (42%) of the custodians with automated records provide copies of records on computer tape or diskette.

---

[59] U.S. Congress, Office of Technology Assessment, Science, Technology and the First Amendment, OTA-CIT-369 (Washington, D.C.: U.S. Government Printing Office, January, 1988) p. 10.

EXHIBIT 4-1

Methods By Which Public Record Custodians Provide Copies of Automated Records



Many companies engage in the commercial dissemination of information, much of which is government information and public record. For example, Mead Data Central, Inc., specializes in legal research services and offers a database called "LEXIS" containing most state statutes and case law. West Publishing Company provides "Westlaw", an on-line information system with case law from all 50 states and the federal government available on-line for a fee. Representatives from both of these companies testified at the Committee's public hearing as to their desire for complete access to public records in electronic formats.

CompuServe, Inc., a private information services network, currently has contracts with Florida's Department of State and Department of Highway Safety and Motor Vehicles to provide access for a fee to particular records which are in high demand by certain businesses. In Lee County, Florida, the property appraiser sells various tapes of databases to two local Boards of Realtors. The Boards contract with a private software vendor to reformat the data to make it more useful to realtors. Then the Boards, for a fee, provide access to the information to any subscriber. Only 2 percent of the survey respondents (7 individuals) indicated that they have entered into an agreement or contract with a private-sector firm to market the electronic access to their public records. However, in each of those cases, the information being disseminated is considered valuable and a market exists for its purchase.

Although the benefits of the private sector information industry are apparent, a recent incident illustrates why, in some cases, the government should be the sole disseminator of certain public record

information. The incident involved an individual requesting a copy of the Florida Department of Law Enforcement's entire criminal history records database on magnetic tape, with bi-monthly updates. The individual, who represented the Merchant's Association of Florida, Inc., wished to market this information to businesses conducting background checks on prospective employees. The department stated that data base transfers of criminal history records could be provided only if the names of individuals were not disseminated. Because the names would be released, the department would not allow such access primarily due to problems of ensuring accuracy. Their administrative rules state in part,

> (3) Copies of records made available to the public ... shall be prominently annotated to indicate whether the record is based upon positive identification using fingerprints . . .
>
> (4) The public is advised that criminal history record checks conducted without the use of fingerprint identification procedures are unreliable.[60]

There are other difficulties in ensuring the accuracy of those records. The Department stated in its written response to the Merchant's Association request that the Department receives approximately 150 seal or expunge orders every week, together with frequent corrections and updates. The Department argued that the law, while guaranteeing that these records are open, also requires their accuracy, since the potential damage to an individual from inaccurate information could be great. Thus, only the Department of Law

---

[60]Rule 11C-6.003, Florida Administrative Code.

Enforcement may disseminate criminal history record information, since it alone can verify the accuracy of its records.[61]

The general counsel for the Information Industry Association (IIA) testifed at the Committee's Ft. Lauderdale public hearing. The IIA represents private, for-profit information services companies, such as Mead Data Central. The IIA believes that government should only disseminate information in non-value-added formats. It argues that an on-line electronic access system provides a valued-added service which should only be provided by the private sector. Although this position has no clear constitutional or statutory basis, the President's Office of Management and Budget, during the Reagan administration, favored a policy of privatization, and Circular A-76 strongly favored the use of the private sector for all functions.[62] OMB Circular A-130, reinforcing this policy, states that "maximum feasible reliance on the private sector" also applies to federal agency information dissemination programs.[63] As a result of OMB's policy position, the National Technical Information Service (NTIS), of the U.S. Department of Commerce, adopted a policy of not competing with private sector software vendors. The NTIS provides on-line access to highly specialized data bases processed by federal agencies,

---

[61]Letter from FDLE to Mr. Roger Westerlund, July 21, 1988.

[62]Office of Management and Budget, Performance of Commercial Activities (Circular No. A-76, August 1983) p. 1.

[63]Office of Management and Budget, Management of Federal Information Resources (Circular No. A-130), Section 7c, 50 Fed. Reg. 52729 (December 24, 1985).

but only when a comparable service is not provided by the private sector.

The Congressional Office of Technology Assessment, in its study of federal information dissemination policies, Informing the Nation, noted that both the information industry and OMB "support government dissemination of Federal information in raw electronic form without software enhancements or searching aids, but oppose government dissemination of enhanced or 'value-added' information."[64] That policy, OTA concludes, conflicts with the federal government's traditional role in disseminating paper documents in other than "raw data" forms. Given the historical and public policy basis for government information dissemination, the OTA report supports extension of that policy to data in electronic formats. Fred Wood, Project Director for the OTA study, stated at the Committee's January 19, 1989 public hearing that "the concept of multiple levels of value-added (services) may be viable, with the private sector frequently providing additional levels of value or enhancement beyond those provided by the government."

What is lacking at both the federal and state levels, however, are guidelines for electronic information dissemination. Such guidelines would assist public records custodians in the performance of their duties while balancing private sector concerns about a government monopoly on information dissemination. Although agencies are required by Chapter 282, F.S., to plan for their computer

---

[64]U.S. Congress, Office of Technology Assessment, Informing the Nation, p. 7.

applications, they are not required to address in their plans how the information will be disseminated, if at all.

Some argue that government must always retain the function of disseminating information, while not restricting others from also doing so. To do otherwise is to threaten democracy since only "profitable" data would be made available to the general public. A commentator recently noted:

> In this information age, the advantaged become more so, and the disadvantaged fall from the back. Life is increasingly regressive because the benefits of information are distributed disproportionately to those already favored by many advantages. The more certain kinds of information matter, the more unequal society---life---becomes.[65]

Summary

Historically, democratic governments have disseminated information as one of their primary functions. However the private sector information industry is growing rapidly and calling into question the government's role in disseminating information.

An informed citizenry is a basic element of democracy. Florida provides its citizens the opportunity to stay informed via laws which guarantee open records, open meetings, provide for public libraries as depositories of public documents, and require the printing of annual reports of government programs.

Many private corporations engage in the dissemination of public information. Although the public may benefit from private sector

---

[65]George Will, "Two-tier drug culture is emerging," Tallahassee Democrat, January 8, 1989.

information dissemination, in some cases, such as with criminal history records, government must remain the sole disseminator of public records. It is, however, often difficult to draw the line between the types of information the government should disseminate and the types it should contract or leave for others to develop and disseminate on their own or under contract. Some argue that government must always retain the function of disseminating information. To do otherwise would threaten the ability to have an "informed public" and could result in the dissemination only of "profitable" data by the private sector while other information is not made available at all.

CHAPTER 5 - COMPUTER SOFTWARE ISSUES

Background

The federal Copyright Act explicitly prohibits the federal government from holding copyright in its works, stating, "copyright protection under this title is not available for any work of the United States Government. . . ."[66] The only exception to this rule emerges when a copyrighted work becomes government property "by assignment, bequest, or otherwise."[67] The federal Copyright Act does not specify whether state governments may hold copyright in their works; therefore, states are free to devise their own laws regarding copyright of state and local government works.

The ability to copyright internally-developed software is a pressing issue in Florida. Metro-Dade County is currently copyrighting and marketing its software, and other counties are interested in marketing their internally-developed software. These counties view the marketing of software as an opportunity to recoup their software development costs and make a profit on their investment of taxpayer funds. Metro-Dade relies upon its General Counsel's written opinion for its authority to copyright. (Copy included in the Appendices.)

---

[66] 17 U.S.C.S. s.105 (1976).

[67] Id.

However, the law in Florida regarding agency copyright is neither unified nor settled. Current statutory authorization for the government to hold copyright exists in the following specified areas:

1) Department of State, ss. 286.021,.031, F.S. - The legal title and every right, interest, claim or demand of any kind in and to any patent, trademark or copyright, or application for the same, now owned or held, or as may hereafter be acquired, owned and held by the state, or any of its boards, commissions or agencies, is hereby granted to and vested in the Department of State for the use and benefit of the state; and no person, firm or corporation shall be entitled to use the same without the written consent of said Department of State.

2) State Universities, s. 240.229, F.S. - In their own name, the universities may secure "letters of patent, copyright, and trademarks on any work products and to enforce its rights therein."

3) Department of Education, ss. 233.25,.255 F.S. - When educational materials are developed by the Department of Education and subject to copyright, patent or trademark they will be available to other appropriate persons in the state educational system.

4) Citrus Department, s. 601.101, F.S.- The department is authorized to obtain patents, trademarks, copyrights or other rights, and may receive and dispose of royalties.

5) Community Colleges, s. 240.319, F.S. - Each community college district board of trustees is authorized to prepare work products related to educational endeavors which are subject to trademark, copyright and patent laws. The boards are required to consider the relative contribution of employees in the development of such products and to enter into binding agreements with them to establish their percentage of ownership. In addition, the boards may secure and enforce letters of patent, copyright and trademarks.

6) Cooperative Marketing Associations, s. 618.07, F.S. - The associations are authorized to establish, secure, own, and develop patents, trademarks and copyrights.

7) Lottery s. 24.105(12), F.S. - The Department of the Lottery is authorized to hold copyright, trademarks, and service marks and to enforce its rights with respect to them.

8) Institute of Phosphate Research, s. 378.101, F.S. - The Institute is authorized to secure patents, copyrights or trademarks and must consider the contribution of its personnel, contractors, and grantees and enter into

agreements to establish their interests.

9) Real Estate Commission, s. 475.04(3), F.S. -
The commission may also publish and sell, at a reasonable price intended to cover costs, a handbook on this chapter and other publications intended to be textbooks or guidelines for study and guidance of students, applicants, licensees, and members of the general public, copyright of which shall be the property of the state.

Discussion

The term "public records" is defined in s. 119.011, F.S. as:

> All documents, papers, letters, maps, books, tapes, photographs, films, sound recordings or other material regardless of physical form or characteristics, made or received pursuant to law or ordinance or in connection with the transaction of official business by any agency. (Emphasis added.)

Construing this definition, the court, in Shevin v. Byron, Harless, Schaffer, Reid and Associates, Inc. held "that a public record . . . . is any material prepared in connection with official agency business which is intended to perpetuate, communicate, or formalize knowledge of some type."[68] The court cited inter-office and intra-office memoranda as examples of public records. Although such memoranda are not a part of the "formal public product, (they) would nonetheless constitute public records inasmuch as they supply the final evidence of knowledge obtained in connection with the transaction of official business."[69] Computer programs are, arguably, public records under this definition. Support for defining software as a public record is also found in s. 119.07(3)(r), F.S., wherein

---

[68] 379 So.2d 633, 640 (Fla. 1980).

[69] Id.

"sensitive" agency-produced software is exempted from the inspection and copying provisions of the Public Records Law. Since government records are presumed open absent a specific exemption, it follows that non-sensitive agency-produced software is subject to the the inspection and copying provisions in the law.

One court has analogized computer software to a code. It would be unreasonable to give a person a message in code without supplying a code book to decipher the message, and it would be equally unreasonable to provide public records without supplying the program to access them.[70] One appellate court has held that although agencies are not required to provide programs to individuals requesting information in specialized formats, they must provide the programs that they have available. The draft security standards promulgated by the Information Resource Commission acknowledge this and state that programs written by employees may be distributed to outsiders if they are public records.[71]

Once a document is classified as a public record, it must remain open for public access, absent clear statutory provisions to the contrary. Thus, documents may be withheld from public inspection only if statutory law provides that they are confidential or if they are

---

[70]See State ex rel. Davidson v. Couch, 117 Fla. 609, 158 So. 103 (1934) cited in Seigle v. Barry, supra at 66.

[71]Florida Information Resource Commission, Draft Information Security Standards and Guidelines, (Tallahassee, Florida: July 7, 1988) p. 10.

expressly exempted by general or special law.[72] The judiciary's only role is to strike a balance between assuring an informed public and permitting the government to maintain secrecy in the public interest.[73] However, courts may not balance policy questions such as the relative significance of the public's interest in a document versus the damage which may result from the disclosure of such document without statutory exemption.[74] Neither may they consider the presence or absence of public demand for a public record in their analysis.[75] If software is classified as a public record, current policy and law require that it be treated as any other public record. It must be made available for inspection without charge and copies must be provided for the cost of duplication.

Additionally, the purpose for an individual's inquiry is immaterial to the issue of determining access to public records.[76] Therefore, a commercial purpose for the request does not prevent the disclosure. Attorney General Opinion 88-23 acknowledges these fundamental principles. Videotapes of training sessions, produced by a state attorney's office, were determined subject to public

---

[72] Section 119.01, F.S.; Rose v. D'Alessandro, 380 So.2d 419 (1980); Wait v. Florida Power & Light Co., 372 So.2d 420 (1979).

[73] See Lorei v. Smith, 464 So.2d 1330 at 1332 (Fla. 2d DCA 1985), pet. for rev. den'd, 475 So.2d 695 (Fla. 1985).

[74] News-Press Publishing Co. v. Gadd, 388 So.2d 276 at 278 (Fla. 2d DCA 1980), See also, ss. 119.01-.07(3)(a), F.S.

[75] Id.

[76] Lorei v. Smith, supra at 133, See also News Press Publishing Co. v. Gadd, note 74 supra.

disclosure in the absence of a statute making the information contained therein confidential. In sum, government documents defined as public records are presumed subject to disclosure absent a clear legislative showing to the contrary.[77] The court can determine when existing statutory exemptions apply to government records, but it cannot create new exemptions.

Consistent with statutory and common law, Attorney General Opinion 86-94 concluded that "unless legislatively or judicially determined otherwise, the clerk of the circuit court does not have the authority to copyright computer programs for certain financial and accounting functions developed by his staff."[78]

The statutes, case law, and Attorney General Opinions indicate software created by public employees, if not "sensitive", are public records, subject to inspection and copying. However, some Florida agencies have copyrighted and sold their software. Metro-Dade has established a separate marketing department to sell not only its software but also its computer-related services. In the Committee's survey, nine agencies indicated they had copyrighted some of their agency-produced software, and fourteen indicated that they had sold some of their software. In most cases, these are local government agencies.

Individuals who testified at the Committee's public hearings voiced concerns about what they viewed as inequities in the situation.

---

[77] See Ely v. F.B.I., 781 F.2d 1487 (11th Cir., 1986).

[78] AGO 86-94 at 237.

They believe it is unfair for certain jurisdictions to spend "millions" of dollars developing software and then "give it away" for free to others. They would like other agencies or individuals to pay for the value of the record, rather than the cost of duplication, so that the agency that develops the software can recoup its costs and make a profit for its taxpayers. Otherwise, they testified, the larger more advanced agencies may end up subsidizing others which are slower to automate, by providing free software.

Other states' laws support this viewpoint. Minnesota authorizes units of government to patent, copyright, and market its software for profit. In 1984, the Minnesota Legislature authorized (MN Stat. s. 375.85) a county or group of counties acting jointly to market their self-developed or vendor custom-developed computer software products or systems. Prices for the software not only include the actual cost of production, but may be based upon market considerations. Counties may also enter agreements with entities in the private sector to assist in marketing their software. A private firm has bought the rights to market and improve a Hennepin County, Minnesota, staff-produced software package and pays the county royalties on its sales. As of February, 1988, the county generated $500,000 for its general fund through the sale of these software packages. The county expects sales of 2 million dollars over the next five years. One of the more recent sales was to the St. Lucie County, Florida, Property Appraiser's Office.[79]

---

[79]"Hennepin County Legacy Continues", Government Technology. January/February 1989, p. 26.

Six other states exempt computer programs from their public records act: Kansas, Oklahoma, Oregon, Utah, Virginia and Wisconsin.[80] The exemption provided in Utah, however, is only for those programs which would jeopardize the security of systems. This is similar to Florida's exemption for "sensitive" software.

If Florida agencies were statutorily authorized to copyright and sell their own software, concerns about the government competing with private sector software developers would emerge. Encouraging or allowing such competition would divert agencies from their public service goals. If software marketing becomes an approved activity, the agency may invest more resources in software development to offset budgetary decreases, without regard for the jurisdiction's need for the program. If the government were authorized to develop and market software programs, resources could be consumed on entrepreneurial ventures, resulting in decreased expenditures in vital areas of public administration and service. For example, Metro-Dade employees will go to a computer center in another state to install a computer program and will support any programs sold by making available maintenance or program enhancements.

Public and private partnerships, similar to Minnesota's example, may result in improved and less costly software programs for the state. Private software companies' portfolios are also enhanced by innovative software packages developed by the state. Florida

---

[80]Office of the Massachusetts Secretary of State, Public Records Division, Report of the First National Conference on Issues Concerning Computerized Public Records, (Boston, Massachusetts: Vol. 2, Appendix, September 1986) p. 9.

Children's Medical Services (CMS), a program of the Florida Department of Health and Rehabilitative Services (HRS), entered into an agreement with Applied Interactive Technologies (AIT) to revise a software program developed by CMS. The software is used to train staff for the many diverse programs CMS offers. The courseware was developed in response to problems such as shrinking travel budgets, lack of standardization among the training programs, and the participants' varied training needs. Florida TaxWatch found the CMS software to be on the leading edge of training strategies. Once sales of the revised software reach the break-even point, the state will receive quarterly royalties. The revenue generated is intended to provide increased and improved services to Florida's children in a time of budgetary cutbacks. Additionally, if the courseware is a marketing success, CMS will receive other revenues in the form of equipment, service or a cash share in the profits. If the software sales are lower than anticipated, CMS will not have to pay AIT for the revised software.

Florida law distinguishes between proprietary software and government-developed software. Florida does not permit government-developed software to be copyrighted, and therefore all such software is subject to public scrutiny unless it is "sensitive". On the other hand, copyright and trade secret laws limit public access to proprietary software, even when that software is owned by the government. This distinction impairs citizens' ability to know about their government and could encourage the purchase rather than creation of some programs to avoid public disclosure.

The private sector is decreasing its use of employee-written software, although not due to disclosure issues. A recent nationwide

survey of large companies reveals that they are relying more on existing software packages and modifications to those packages to meet their needs, rather than creating their own software. Forty-four percent of the major applications of those large companies were reportedly purchased packages.[81]

Proprietary software, which state government purchases from private vendors, is protected by an exemption from the Public Records Law in s. 119.07(3)(r), F.S., if it is considered a trade secret. The public may neither view nor copy such software. This exemption was added by legislation in 1985 to protect the vendors' trade secrets.[82] Under the Public Records Law, copyrighted software may be inspected but not copied. The public access to software, however, is inconsistent because there are no laws regulating which software should be purchased and which software should be created.

The status of copyrighted software used by a state government has been questioned in a California court case which may have significant implications for Florida. In BV Engineering v. University of California, Los Angeles,[83] a software development firm sued the university for making unauthorized copies of copyrighted software. The U.S. Court of Appeals ruled that the state could not be sued for

---

[81] "Business Squeeze Pushes Software Sales Up 184%", Computerworld, August 22, 1988, p. 55.

[82] Trade secrets are formulas or compilations of information which are unique and give one an advantage over others who do not know it. This is distinguished from copyright protection, in that a copyright does not extend to the ideas or patterns or formulas embodied in a work.

[83] 858 F.2d 1394 (9th Cir. 1988).

violating the Federal Copyright Law because the Eleventh Amendment to the United States Constitution precludes a state from being tried in federal court absent a waiver of immunity. California has not waived its immunity in this area, and neither has Florida. Therefore, the government may be immune from suit if it copies copyrighted software or violates any other copyright law.

The UCLA case, if followed in Florida, would create a gap in the protection for certain kinds of proprietary software: trade secret software is exempt from the inspection and copying provisions of Chapter 119, F.S.; copyrighted software is not. This lack of protection for copyrighted software could severely impact the sales of such software to public agencies in Florida.

The concept of protecting software is questioned by Richard Stallman, a computer programmer at M.I.T. He develops sophisticated software which he gives away for free. He believes that software should not receive the same protections as other physical commodities, since it costs so little to copy. His philosophy is that information, including computer programs, should be shared. Mr. Stallman's software comes bundled with one of the newest computers on the market and he has received support from major computer corporations for his work.[84]

The federal government has a similar approach. The Office of Data Base Services of the National Technical Information Service (NTIS), Department of Commerce, sells over 500 different,

---

[84]John Markoff, "A Battle to Make Software Free," The New York Times, January 11, 1989.

non-sensitive computer programs created and used by the federal government. NTIS is self-supporting, and thus the price of the computer programs includes administrative, overhead and actual duplication media costs. Agencies are allowed to determine a market value for the software. Those values range from $150 to $1,925 for the majority of software and data files. A few of the products are priced higher and are governed by contracts for use. This program benefits agencies by decreasing the time and money spent on programming and developing systems already available. Mr. Lee Holroyd, the Information Systems Director for the City of Ft. Lauderdale, recommended, at the Committee's Ft. Lauderdale public hearing, that the state adopt a similar clearinghouse approach.

A number of state and local governments already participate in software exchange programs. Pinellas County provides copies of its software for its integrated criminal justice system to other government agencies for the cost of duplication. According to the 1986-87 Annual Report of the National Association of State Information Systems, there were 91 transfers of software between the states reported between 1974 and 1987. The types of programs shared ranged from unemployment benefits software to surface mining programs. Florida was listed as the beneficiary in two of the transfers.[85]

---

[85]National Association of State Information Systems, Information Systems Technology in State Government, (Lexington, Kentucky: 1987) pp. 35-36.

Summary

The federal Copyright Act explicitly prohibits the federal government from holding copyright in its works, but does not specify whether state governments may hold copyright in their works. Florida law permits the state and certain agencies to hold copyrights in specified instances. Some local governments in Florida are particularly interested in marketing their internally developed software as a means to recoup some of their software development costs and make a profit for their taxpayers. Existing statutory law, case law, and attorney general opinions indicate that software is a public record and therefore subject to the inspection and copying provisions of Ch. 119, F.S., unless it meets one of the statutory criteria for exemption. However, Metropolitan Dade County is selling internally developed software for profit.

In Florida, it is not unusual for agencies to use two types of software: that which they create and that which they have purchased through a licensing agreement from a private sector software firm. This means that under the current law those agencies use some software which is subject to the inspection and copying provisions of the Public Records Law and also use some which is exempt from those provisions. This inconsistency affects the public's ability to know about its government, how it functions, and how certain decisions are made. The states immunity from suits in federal courts further complicates the status of copyrighted software.

If government-produced software were statutorily exempt from the inspection and copying provisions in current law, concerns may be raised about government competing with the private sector software

developers. The federal government authorizes agencies to send copies of their software to the National Technical Information Services, a branch of the Department of Commerce, which acts as a clearinghouse for federal agencies' internally created software. Many states participate in exchanges of software with other states and the federal government.

CHAPTER 6 - COMPUTER MATCHING

Background

Computer matching is the computerized comparison of two or more automated systems of records to identify individuals common to two or more of the record systems or unique to one of the record systems. Matching is used to check for persons who should not appear in two record systems, as in the case of recipients of food stamps and government employees who earn above a certain salary. Matching is also used to locate those who should appear in two record systems, but do not, such as males registered for the military draft and males between the ages of 18 and 26 with drivers licenses. Computer matching is one of several techniques developed to screen, edit, and scan data to identify irregularities that may indicate fraud, abuse, or error in government activities.

The rapid development of computer technologies has enhanced the ability to match records. This, in turn, has increased the government's use of computer matching dramatically. In little more than a decade, computer matching has become a major federal activity, and both the executive and legislative branches have encouraged its use. Proponents consider it an effective tool for improving the integrity of benefit programs. Critics argue that matching raises serious concerns about Fourth Amendment rights, privacy rights, cost-effectiveness, and computer linkages that may lead to a centralized data base.

"Project Match" was initiated in 1977 by the U.S. Department of Health, Education, and Welfare to match AFDC records with payroll

records of federal workers. This effort was the first major federal program which utilized computer matching to combat fraud, waste, abuse, and error in government programs. Following "Project Match", federal agencies adopted computer matching as an ongoing management tool.[86] In 1981, President Reagan established the Council on Integrity and Efficiency. A major project of the Council was a long-term computer matching program designed to facilitate and improve computer matching in federal and state governments for broad management purposes, rather than exclusively to combat fraud and abuse.[87]

The states' use of computer matching is greater than that of the federal government. Computer matches are conducted by at least four-fifths of the states. Most of these matches are performed in response to federal direction, and most matching occurs in federally funded programs or those controlled by federal law.[88] Public Law 95-216 requires states to match AFDC cases against state wage information, and Public Laws 96-249 and 97-98 require states to disclose wage and unemployment compensation information to food stamp agencies for use in computer matching. The Deficit Reduction Act of 1984 requires states to develop an income and eligibility verification

---

[86]U.S. General Accounting Office, Computer Matching - Assessing Its Costs and Benefits, GAO/PEMD-87-2 (Washington, D.C.: U.S. Government Printing Office, November 1986), p. 18.

[87]Id.

[88]U.S. Congress, Office of Technology Assessment, Federal Government Information Technology: Electronic Record Systems and Individual Privacy, p. 59.

system to permit comparison of records in AFDC, Food Stamp, Medicaid, and other related programs. Wage, asset, and other information from the Social Security Administration and the Internal Revenue Service are to be made available to state agencies that determine eligibility for various welfare programs for verification purposes. In addition, standardized formats are to be developed for data exchange.[89] In Florida, the Department of Health and Rehabilitative Services is planning to implement an automated information system which will enable the Department to meet the provisions of The Deficit Reduction Act and other federal legislation.

Until the present time, there have been few, if any, controls on matching in the federal and state governments. However, increasing public concern about the privacy implications of computer matching led to the enactment in October, 1988, of Public Law 100-503, The Computer Matching and Privacy Protection Act. This law will regulate matching programs conducted by federal agencies or by other agencies using federal records, including state agencies.

Discussion

Many Florida agencies use computer matching. State agencies match records with federal and local agencies, and with private sector organizations, such as banks. In the Joint Committee on Information Technology Resources' 1988 survey of Florida state agencies, eleven out of 26 respondents indicated their agency conducted computer

---

[89] U.S. General Accounting Office, Computer Matching - Assessing Its Costs and Benefits, p. 19.

matching activities during the 1987-88 fiscal year. Four of the eleven agencies also participated in front-end verification, a type of computer matching where the accuracy and authenticity of information supplied by an applicant for government benefits, employment, or services is checked against similar information from another agency or source. (Please see Exhibit 6-1.) Front-end verification is not examined in this report, since its use is still rather limited in state agencies.

The total estimated number of records matched by the eleven agencies during 1987-88 was over 18 million. Six departments responded that during the year they had participated in 1 to 5 matches; two departments participated in 6 to 10; and one department participated in 11 to 15 matches. Additionally, five divisions of the Department of Education and three divisions of the University of Florida participated in 1 to 5 matches each, and one University of Florida division participated in more than 15 matches. Florida State University reported 1 to 5 matches during 1987-88.

Six of the eleven agencies that conduct computer matching reported that some of their matches are required or authorized by state or federal law. The Department of Health and Rehabilitative Services conducted 14 matching programs in 1987-88; six of these were authorized or required by federal law, and eight by state law.

Public concerns about efficiency in government promote the use of computerized matching to reduce fraud, abuse, and waste. In Florida, as elsewhere, these concerns have grown in response to funding

EXHIBIT 6-1

STATE DEPARTMENTS WHICH PARTICIPATED
IN COMPUTER MATCHING AND FRONT-END VERIFICATION
ACTIVITIES DURING 1987-88 FISCAL YEAR

Department	Participated in Computer Matching in FY 1987-88	Participated in Front-End Verification in FY 1987-88
Administration	X	
Agriculture & Consumer Services		
Banking & Finance		X
Business Regulation		
Citrus		
Commerce		
Community Affairs		
Corrections	X	
Education	X	
Environmental Regulation		
Executive Office of the Governor		
Game & Fresh Water Fish Commission		
General Services		
Health & Rehabilitative Services	X	X
Highway Safety & Motor Vehicles	X	
Insurance & Treasurer	Did not respond	Did not respond
Labor & Employment	X	
Law Enforcement	X	
Legal Affairs	Did not respond	Did not respond
Lottery	X	
Military Affairs		
Natural Resources		
Parole & Probation		
Professional Regulation	Did not respond	Did not respond
Revenue	X	
State		
State Board Administration		
State University System	X (FSU & UF)	X (UF)
Transportation	X	X

11 out of 26 responding state departments participated in computer matching.
4 out of 26 responding state departments participated in front-end verification.

reductions and tighter control of resources. Technological developments now allow easy comparison of large sets of data. With the newer technologies, data is moved more easily and efficiently across organizations and matched with data from different programs and files.

In Florida, the most commonly used method of exchanging records with another agency is exchange of computer tapes. All state agencies which participate in computer matching use this type of record exchange as one of their methods. Three departments use on-line exchange and two departments either exchange hard copy or floppy disks.

Justification for matching includes tracking down those who refuse to pay child support, detecting welfare fraud, and establishing law enforcement information systems. Other potential benefits are collection of overpayments and debts, deterrence of fraud and abuse, and increased public support for programs. Matching proponents argue that computer matching benefits the agencies, their clients, and the general tax-paying public.

Opponents of matching criticize the technique as unproven, ineffective, illegal, and violative of privacy rights.[90] Because nearly everyone may be subject to computer matching without their consent or knowledge, computer matching raises a number of questions and concerns. Many questions regarding legal and constitutional

---

[90]U.S. House of Representatives, Computer Matching and Privacy Protection Act of 1988 (H.R. 4699) Report, (Washington, D.C.: July 27, 1988), p. 3.

issues (such as unreasonable searches and seizures, due process, and the presumption of innocence) surround the use of computer matching in government benefit programs. Questions also arise whether matching is cost effective and whether the matches achieve the cost-savings or cost-avoidance anticipated. A 1986 General Accounting Office study of costs and benefits of computer matching in federal agencies concluded that there was no established methodology for performing cost-benefit analyses of computer matching and that most cost-benefit assessments were incomplete, not reported in monetary terms, or both.[91] Federal agencies made matching decisions informally, and the issue of cost effectiveness was not one of the major factors in making the decision.[92] Generally, proposed matches were not considered in dollar costs, but in agency resources, such as staff and materials required to plan and conduct the match.[93]

The Joint Committee's survey of state agencies revealed that only four of eleven agencies conducting computer matching performs any cost-benefit analyses, and only one entity (a division within a state university) indicated it always performs a cost benefit analysis prior to and after a match. Only three of the eleven agencies could provide

---

[91]U.S. General Accounting Office, Computer Matching - Assessing Its Costs and Benefits, pp. 78,79.

[92]U.S. House of Representatives, Hearing Before a Subcommittee of the Committee on Government Operations - Computer Matching and Privacy Protection Act of 1987 (s.496), (Washington, D.C.: 1987), p. 66.

[93]U.S. General Accounting Office, Computer Matching - Factors Influencing the Agency Decision-making Process, GAO/PEMD-87-2, (Washington, D.C.: U.S. Government Printing Office, November 1986), p. 18.

any figures on the average cost of matching programs and the average amount of money saved or recovered in 1987-88 through matching. However, two of the three agencies providing dollar amounts indicated they never performed cost benefit analyses on matches.

The Florida survey indicates that only one department and one division within a university always obtain written consent from the subjects prior to a computer match. One department and one division of the Department of Education indicated they sometimes get written consent, and the other departments said they never get such consent.

The costs to the clients of benefit programs may be an invasion or loss of privacy, loss of control over personal information they give to state agencies, or termination of benefits based on erroneous information. Using personal information in a computer match has been viewed as an invasion of privacy, especially when individuals are not aware that files containing their identifying information are being used.

Some individuals are concerned about using personal information for purposes other than those for which the information was originally collected. Concerns about a national data base and citizen identification numbers have reemerged because data file linkages have created a de facto national data base. The ability to create this ad-hoc data base grows as federal and state governments collect, maintain, and use increasing amounts of personal information in machine-readable form. These concerns may result in discouraging potential clients from seeking program benefits to which they are legitimately entitled.

In introducing to the U.S. Senate legislation to regulate computer matching activities, Senator William Cohen stated:

> Computer matching programs, unless properly conducted and controlled, can pose serious threats to the privacy and due process rights of individuals whose records are matched...In matching programs, individuals can have crucial government benefits reduced or terminated solely on the basis of unverified information produced by a computer match--information that can be out-of-date, misleading, or just plain wrong. Citizens can be--and have been in the past--placed in the difficult position of having to defend themselves against information that has never even been reviewed by a human being for its accuracy.[94]

Prior to the passage of Public Law 100-503, the Computer Matching and Privacy Protection Act in October, 1988, few, if any limits had been placed on computer matching. The disclosure restrictions of the federal Privacy Act have been interpreted by the Office of Management and Budget and other agencies to allow the disclosures necessary for computer matching.[95] Because the Privacy Act was enacted when most government information was on paper, many individuals are recommending that the Act be reexamined in the context of the computer and telecommunications age. Few state or federal laws provide policy guidelines on computer matching and only slight oversight or follow-up occurs for those that do exist. The Joint Committee on Information Technology 1988 survey of Florida agencies indicates that nine of eleven state agencies conducting matching programs have implemented at least some policies and procedures to regulate these activities.

---

[94]U.S. Congressional Record, August 14, 1986, p. S11746.

[95]U.S. House of Representatives, Computer Matching and Privacy Protection Act of 1988 Report, House Report No. 100-802, 100th Congress, 2d Session, (Washington, D.C.: July 27, 1988), p. 5.

However, there is no state statute which uniformly regulates computer matching in Florida agencies and consequently no explicit legislative oversight of matching activities.

The need for due process in computer matching was demonstrated by a match conducted in Massachusetts in 1982. In order to identify welfare recipients who had more assets than permitted by law, the state matched welfare records against the account records of private banks. More than 1,600 recipients were found to have excess assets and were automatically sent termination of benefits notices. The information used in the match was neither confirmed nor verified, nor were the individuals contacted before their benefits were terminated. After a much higher than normal rate of appeals, investigation found that 15% of the notices were sent due to incorrect social security numbers. In other cases, money in joint accounts also belonged to the other individual named on the account, or the money was held in trust for others. Some of the funds were held legally, for purposes such as paying funeral expenses.[96]

The Massachusetts example demonstrates that computer data must be verified before a government agency takes any adverse action against an individual. Due process also requires that the individual be notified of any proposed action and be given an opportunity to contest the action. The Florida survey shows that one department and one division in a university had terminated benefits based on erroneous information. Two departments indicated administrative hearings had

---

[96]U.S. House of Representatives, Computer Matching and Privacy Protection Act of 1988 Report, p. 6.

been held concerning action resulting from a matching program. However, to date no one has legally challenged any matching programs in Florida.

The increasing use of computer matching in federal and state governments mandates that standardized due process procedures, administrative controls, and cost-benefits assessments be implemented. The Computer Matching and Privacy Protection Act of 1988 amends the Privacy Act and establishes controls and oversight mechanisms on certain matching activities at the federal level and in other agencies where federal records are involved. This law allows computer matches to continue, but establishes procedures to protect individual rights. Under this legislation, matching programs can only be established by matching agreements, which specify the purpose and plan for the match. Such agreements must be approved by Data Integrity Boards established within the matching agencies. The bill also requires that information resulting from computer matching programs be independently verified before any adverse action is taken. In addition, individuals must be given notice and an opportunity to contest any findings resulting from a computer match. Finally, a Data Integrity Board may not approve any matching agreement unless the agency has submitted a cost benefit analysis of the proposed matching program, demonstrating that the program is likely to be cost effective. Supporters of the law hope that it represents the first step in a larger reform effort to increase the effectiveness of the Privacy Act.

Since much of the matching conducted by state agencies involves federal records, many of these activities will now be regulated by the new federal legislation. However, state matching programs which do

not involve federal records will not be governed by the federal matching law.

Summary

Computer matching is the computerized comparison of two of more automated systems of records to identify individuals common to two or more of the record systems or unique to one of the record systems. The rapid development of computer technologies has enhanced the ability to match millions of records, and government's use of computer matching has increased dramatically.

Few controls on matching had applied to federal and state governments, before October, 1988, when Public Law 100-503, the Computer Matching and Privacy Protection Act, was enacted. It regulates matching programs conducted by federal agencies or by other agencies using federal records, including state agencies.

Florida agencies computer match extensively. In a 1988 Joint Committee on Information Technology Resources survey, 11 state agencies responded that they had matched, during the previous year, an estimated total of over 18 million records.

Using computerized matching to increase the efficiency of government programs is supported by both improved technology and decreasing resources. In Florida, as elsewhere, the concern over fraud, abuse, and waste in government programs has grown in response to funding reductions and tighter control of resources. Technological developments now allow easy comparison of large sets of data.

No state law uniformly regulates computer matching in Florida agencies and consequently no legislative oversight of such activities exists.

CHAPTER 7 - FAIR INFORMATION PRACTICES

Background

Government computers store large amounts of personally identifiable information. This information is readily combined and used in making decisions about individuals, as in computer matching and front-end verification programs. It is becoming increasingly difficult to know where personal information is stored, to know how to access it, and to assure that it is correct.

The federal Privacy Act of 1974 incorporates fair information principles by giving individuals the right to access much of the personal information kept on them by federal agencies. It also places limits on disclosure to others and requires agencies to keep logs of all disclosures of personal information. It gives individuals the right to change incorrect information pertaining to them. Federal agencies may collect only relevant information on individuals, must get the information directly from such individuals where possible, and must notify them of certain facts when the information is requested. A premise underlying the Privacy Act is that information about individuals should not be maintained in secret files; therefore, the agencies are required to publish in the Federal Register an annual report on their systems of records that contain personal information. The report must include a description of the categories of records maintained by the agency, the types of sources for the information, and the purposes of the records.

Florida has not enacted a fair information practices law similar to the federal Privacy Act. Legislative attempts to institute such a

law in Florida have failed for three consecutive years. At the Committee's Ft. Lauderdale public hearing, Alan Westin, Professor of Law at Columbia University, hypothesized why the federal law passed successfully and why attempts at the state level have failed. He noted that the Watergate scandal in the early 1970's raised public consciousness on issues of privacy and public access to government records at the federal level. The media generated additional publicity on these issues and effectively focused attention on the need to pass fair information practices legislation. Westin feels that until an event occurs at the state level to cause the public to call into question the state's handling of public information, Florida may be unable to pass a similar law.

Ten states have enacted fair information practices acts (FIPA). Nine of the ten based their statutes on the federal Privacy Act. These states are Arkansas, California, Connecticut, Indiana, Massachusetts, Minnesota, New York, Ohio, Utah, and Virginia. Minnesota law predates the federal law and is based on data protections established in Swedish law. European countries and Canada have been more concerned about data protection issues and have enacted more legislation than the United States. In the late 1970's, West Germany, France, Norway, Denmark, Austria and Luxembourg passed privacy laws affecting private and public record keeping. In 1978, Canada enacted a human rights provision with privacy protections for federal records.[97]

---

[97]Robert Ellis Smith, Compilation of State and Federal Privacy Laws, (Washington, D.C., Privacy Journal, 1988), p. v.

Although Florida does not have a fair information practices law, several components of such a law are dispersed throughout the statutes. The Public Records Law protects access to information but does not control the access. The security of records is also addressed in the Public Records Law, which makes exposing exempted public records a first-degree misdemeanor. Section 282.318, F.S., the Security of Data and Information Technology Resources Act, provides policy guidelines to the executive branch on the protection of data. Other laws address components of fair information practices, but only for unique types of data, such as fingerprints of child care workers. However, to date some of the other fair information principles have not been addressed in Florida law.

Discussion

All governments collect and use information on individuals in the process of governing. In democratic governments, records must be open to the people, but also must protect individuals' privacy. The federal Privacy Act was passed in 1974 to address this need to collect information and protect the subjects of the information. The Act incorporates accepted standards of fair information practices, governing the collection, use, disclosure, retention, and disposal of personal information. These standards include rights for individuals to:

1. Know what records pertaining to them are collected, maintained, used, and disseminated by government agencies;

2. Have access to personal information that agencies maintain on them and to amend or correct the information;

3. Receive notice regarding certain facts, such as how personal information collected on them by government agencies will be used.

Federal fair information principles establish rights and remedies for individuals who are the subjects of agency information gathering and establish certain requirements for federal agencies to meet in handling personal information. The federal Privacy Act also provides that a government agency can collect only information that is relevant and necessary to the agency's function and must collect information to the "greatest extent practicable" directly from the individual if the information may result in an adverse determination about an individual's rights, benefits, and privileges under federal programs.

The fair information principles contained in the Privacy Act protect personal information in federal records. However, critics of the 1974 law believe it does not provide adequate protection for information abuse and misuse in the information age. In 1974, the authors of the Act did not envision today's distributed processing, sophisticated data base management systems, computer networks, and wide use of microcomputers in government.

As the technologies for telecommunications, networking, and computer systems integration continue to improve, they greatly increase the ability of government organizations to share information with each other. Advances in information technology have aided the collection and use of personal information by the federal and state governments. However, these same advances have made it more difficult to monitor agency information practices and to protect individuals' rights. It is also more difficult for individuals to learn about how their records are being used and to access and amend information on

themselves. Individuals may not be aware that information about them is being used in a computer match or a computer profile.

The increased collection and use of personal information made possible by the changing technologies have resulted in more public support for legislative protections of personal information.[98] People want to be assured that personal information collected or compiled by government organizations will be accurate and relevant, and will not be misused or inappropriately disclosed to others. This protection involves ready access to an individual's own records, security of the information and information systems, ways to inform individuals as to where information is stored and where it has been disseminated, and the ability to correct the information when necessary.

The recently passed federal Computer Matching and Privacy Act of 1988, Public Law 100-503, regulates certain computer matching activities in federal agencies and those state and other agencies utilizing federal records in matching programs. This legislation includes fair information principles, such as giving notice to individuals on the use of their personal information in a matching program and requiring that the personal information used in computer matches be verified as accurate. In Florida, where the Public Records Law places few limits on disclosure of personal information, it is even more important that such information be accurate and that the

---

[98]U.S. Congress, Office of Technology Assessment, Federal Government Information Technology: Electronic Record Systems and Individual Privacy, OTA-CIT-296 (Washington, D.C.: U.S. Government Printing Office, June 1986) pp. 28,29.

subjects of that information be informed of how it is used and with whom it is shared.

The experiences of other states which have enacted fair information practices legislation, most of which were based on the federal Privacy Act, have varied. All seven states that responded to the Joint Committee survey reported that their laws had been amended in some way. Most of the changes were minor, but several changes were significant, such as eliminating the annual reporting requirement on systems of records, repeal of sections conflicting with a state's Freedom of Information Act, and expanding their law's coverage to include municipalities.

Most of the states were unable to provide any information on important aspects of their laws. For example, only three of the seven respondents could estimate the number of individuals who see their personal information. And only two of seven knew the number of individuals who requested changes to their personal information. Costs to carry out state fair information practices laws have been low. Only two states reported that specific appropriations were made to carry out their laws ($25,000 for start-up in one state, $100,000 annually in the other). Among the five states that were able to calculate costs associated with such laws, annual costs ranged from a low of $1,000 to a high of $500,000 (including costs of both state and local governments).

However, more information was available in other areas. Six out of the seven states indicated that most of their fair information practices disputes are resolved between the agency and the individual and are not appealed to an outside authority. Two of the seven states

had not held any formal hearings to settle disputes; two had held 6 to 10 formal hearings; two did not know whether any formal hearings had been held; and one indicated that formal administrative hearings were not available. Concerning the number of court cases, one state indicated none, three states said between 1 and 5, one state indicated one Supreme Court case, but it was not known if there were any trial court cases. Two states have litigated more than 20 court cases involving their fair information practices laws. However, there is no information that any damage awards were made, as evidenced by the four responses of "none" and three responses of "unknown" to the question regarding such awards.

The survey also provided information about the categories of individuals which generate the highest number of requests and disputes under the other states' fair information practices legislation. The two groups listed most often as generating the highest number of such requests and disputes were prisoners and current or former state personnel, respectively. These groups were exempted from the 1988 Florida Fair Information Practices bill, which was not enacted by the 1988 Legislature.

Most of the states reporting ongoing costs associated with the legislation noted that the major cost was the publication of the annual report. Four states were required to publish reports and three were not. Five states established employee positions in response to the FIPA legislation, and two did not. Of the five, two states indicated between 1-5 positions were established, two indicated one position (one state has since eliminated that position), and one state indicated two positions.

The 1987 Joint Committee Report, Fair Information Practices, discussed the implementation of fair information practices legislation in Minnesota, California, and New York. Interviews conducted in 1988 with officials in those three states provided further information on their states' FIPA activities to date.

Minnesota: The Minnesota Government Data Practices Act applies to state agencies and to political subdivisions. According to the survey response, the estimated statewide cost to comply with the law is $500,000 annually, and most of this cost is associated with personnel time. Two new positions were added to process requests under the Data Practices Act. Much of the work generated by the law results from conducting training programs on compliance for local government personnel.

Minnesota established the Data Privacy Division to function as an informational service for questions about the Data Practices Act. The Privacy Division reports that few formal hearings are heard each year, and informal disputes average about 100 a year. Since the act's implementation in 1974, there have been a number of court cases. The issues in these cases have dealt with either access to information or correction of personal information or both.

In Minnesota, the information disputes fall into three main categories, in the following order:

1) State and local government personnel;
2) Welfare area - especially cases challenging determinations relating to child abuse reports;
3) Prisoners.

The legislation has been amended since its implementation. The annual reporting requirements have been repealed, because they were too costly and burdensome for both the state and local government

agencies. A second change narrowed the "notice to individuals" requirement, and notice is now given only when private or confidential data is requested by an agency.

California: The California Information Practices Act of 1977 applies to state agencies only. It has been difficult or impossible to obtain data on agency costs to comply with the law. Legislation enacted in 1987 requires that agencies report compliance costs to the state Office of Information Practices. Agency reports indicate that compliance costs vary widely, but the Manager of the Office of Information Practices explains the reported cost data is incomplete and of doubtful accuracy. Legislation has been proposed to eliminate the agency fiscal impact reporting requirement.

Any disputes under the Information Practices Act which cannot be resolved within agencies are heard before the Office of Information Practices. The number of disputes which reach the Office of Information Practices is low. In 1986, there were 22 formal disputes and in 1987, there were 12. The cases primarily involved access and disclosure issues. Other disputes concerned maintenance, collection, and content of information. To date, no disputes have gone to court because of an agency's refusal to change records.

As a group, state government employees provide the largest number of requests and disputes. The next largest category is professional licensees, including doctors, behavioral scientists, social workers, and nurses. Other categories include sales and use tax permit holders, applicants for state employment, former mental patients, labor disputants, former employees, and students.

The legislation has been amended since its implementation, but the changes were mainly for purposes of clarification.

New York: The New York Personal Privacy Protection Law applies to state agencies only. Precise information on the costs to comply with the legislation is not available, but the Director of the Committee on Open Government reports the fiscal impact is minimal. This fact is significant since the current directory published by the Committee identifies 1,948 systems of records maintained by state agencies.

The current annual report to the Governor and Legislature states that in 1987, 3,294 access requests to 65 agencies were made under the Personal Privacy Protection Law. This figure indicates that more than twice as many access requests were made in 1987 than in 1986. In contrast, only 169 requests to amend or correct records were made in 1987, and all were granted. Information on the number of such requests for 1986 is unavailable. More than half of the oral inquiries directed to the Committee on Open Government regarding the Personal Privacy Protection Law were made by state agency officials seeking to comply with the law.

Current state employees comprise the largest category of individuals requesting or challenging personal information. The Personal Privacy Protection Law has been in effect for over three years. Although the legislation has not changed radically during that period, one minor change now permits state agencies to disclose personal information of historical value to state archives, unless it is confidential by statute.

Summary

The federal Privacy Act of 1974 incorporates fair information principles by giving individuals the right to access much of the personal information kept on them by federal agencies, placing limits on disclosure to others, and requiring agencies to keep logs of all disclosures of personal information. It also gives individuals the right to change incorrect information pertaining to them.

Although Florida does not have a fair information practices law, the state has codified several of its components. However, other fair information principles have yet to be addressed in Florida law. Such legislation was introduced during the last three legislative sessions in Florida, but it did not pass.

All governments collect and use information on individuals in the process of governing. In democratic governments records must be open to the people, but also must protect individuals' privacy. Thus, an inevitable tension exists between the freedom of information goals and privacy concerns. Ten states have enacted fair information practices legislation, and their experiences have varied. Their experiences suggest the need to build into such a law criteria for judging success as well as a reporting mechanism for collecting relevant data.

As the technologies for telecommunications, networking, and computer systems integration continue to improve, they greatly increase the ability of government organizations to share information with each other. However, these same advances make it more difficult to monitor agency information practices and to protect individuals' rights. It is also more difficult for individuals to learn about how

their records are being used and to access and amend information on themselves.

In Florida, where the Public Records law places few limits on disclosure of personal information, it is even more important that such information be accurate and that the subjects of such information be informed of how it is used and with whom it is shared.

CHAPTER 8 - TECHNOLOGICAL IMPACTS ON PRIVACY

Background

The conflict between privacy rights and public access to government records is inherent and inescapable: although the conflict can be managed, it will never be solved. Unless information is specifically identified as confidential and exempted from the Public Records Law, it is considered a public record and subject to review. Article I, Section 23 of the Florida Constitution creates a right of privacy, but the constitutional provision does not "limit the public's right of access to public records and meetings as provided by law." Thus, much personally identifiable information kept by state agencies is available for anyone to see.

Florida's Public Records Law may be in conflict with the federal right to disclosural privacy. In Fadjo v. Coon,[99] the United States Court of Appeals for the Fifth Circuit stated, with reference to the Florida Public Records Law: "The legislature cannot authorize by statute an unconstitutional invasion of privacy." The Circuit Court recommended that a balancing approach be used when the state's interest in disclosing information collides with a person's interest in disclosural privacy. The court cited two major problems with the Public Records Law in relation to privacy issues: "It is too broadly drawn, and has been construed to exclude judicial balancing of competing interests."

---

[99] 633 F.2d 1172 (5th Cir. 1981).

The Florida Supreme Court has been reluctant to apply the balancing test in cases where personal privacy has been in direct conflict with the Public Records Law. At this time the right to privacy in Florida is subordinate to the right to access public records.

Discussion

The new computer-based technologies permit rapid accumulation and exchange of personal information on large numbers of individuals. Such massive data collection and dissemination pose the danger of creating personal data composites. Decisions about individuals are made by both the government and the private sectors based on comprehensive "data images" drawn from diverse files serving unique programs and policies. The federal Privacy Act of 1974 restricts the collection, maintenance, use, and dissemination of federal agency records. The purpose of the law is to provide safeguards for individuals to protect personal privacy. It requires federal agencies to establish rules and procedures for maintaining and protecting personal information in agency record systems. This law seeks to balance an individuals right to privacy protection of personal information against the federal government's need to collect and use that information.

When the Privacy Act was enacted, federal agency record systems were still based mainly on paper documents. In the intervening years, advances in computer and communications technology have enabled agencies to collect, use, store, exchange, and manipulate individual records in new ways. Today, the newer technologies are outside the

boundaries of many privacy laws, including the federal law, because the laws either do not exist, the current ones are obsolete, or have not been applied.

The Deficit Reduction Act of 1984 increased the government's collection and use of information on individuals. This Act requires all states to participate in file merging, matching, and linking programs to verify eligibility of beneficiaries in various government programs, such as Food Stamps, Medicaid, and AFDC. In Florida, this and other federal legislation place information gathering requirements on numerous state agencies in areas such as child support enforcement and many need-based and insurance-based programs. Although Florida maintains personal information on millions of its citizens the state has adopted few laws or policy guidelines to govern how information is collected and used.

Computers are increasingly used to certify the accuracy and completeness of personal information before an individual receives a government benefit, service, or employment. Federal and state government agencies collect and use many millions of records containing personal information on individuals. Consequently, possession of such vast quantities of personal information has raised concerns over the ability to protect and balance the privacy of individuals in relation to the information needs of government.

Special privacy concerns are raised by the advances in computer technology. Growth in the scale of computerization, the increase in computer networking and other linkages, the electronic searches of computerized files, and the increased use of microcomputers all

threaten Privacy Act protections.[100] Today's privacy concerns extend beyond unreasonable search and seizure to these other activities. For example, technology allows personal information to be collected in new ways, such as from fingerprinting, lie detectors, urinalysis, and blood tests, including AIDS antibody testing. Genetic screening and testing provide information on individuals by biological characteristics or capabilities. Some of the newer information gathering technologies available to law enforcement include: automated fingerprint identification, electronic monitoring bracelets, biometric security systems (comparison of individual physical traits), telephone taps and recorders, pen registers (which monitor the numbers called, but not the content of calls), and monitors for computer usage and for electronic mail.

Massive amounts of personal information can be compared in an unlimited number of public and private agencies using direct on-line linkages. Computer tapes, software, and networking also make it possible to compare personal information stored in different record systems, thus having the effect of establishing centralized files and data bases. Microcomputers have transformed the modern office and have improved productivity and the capacity to effectively manage government programs. However, this technology places the control of computing in the hands of end-users, who may have access to centralized data bases through telecommunications networks. All of

---

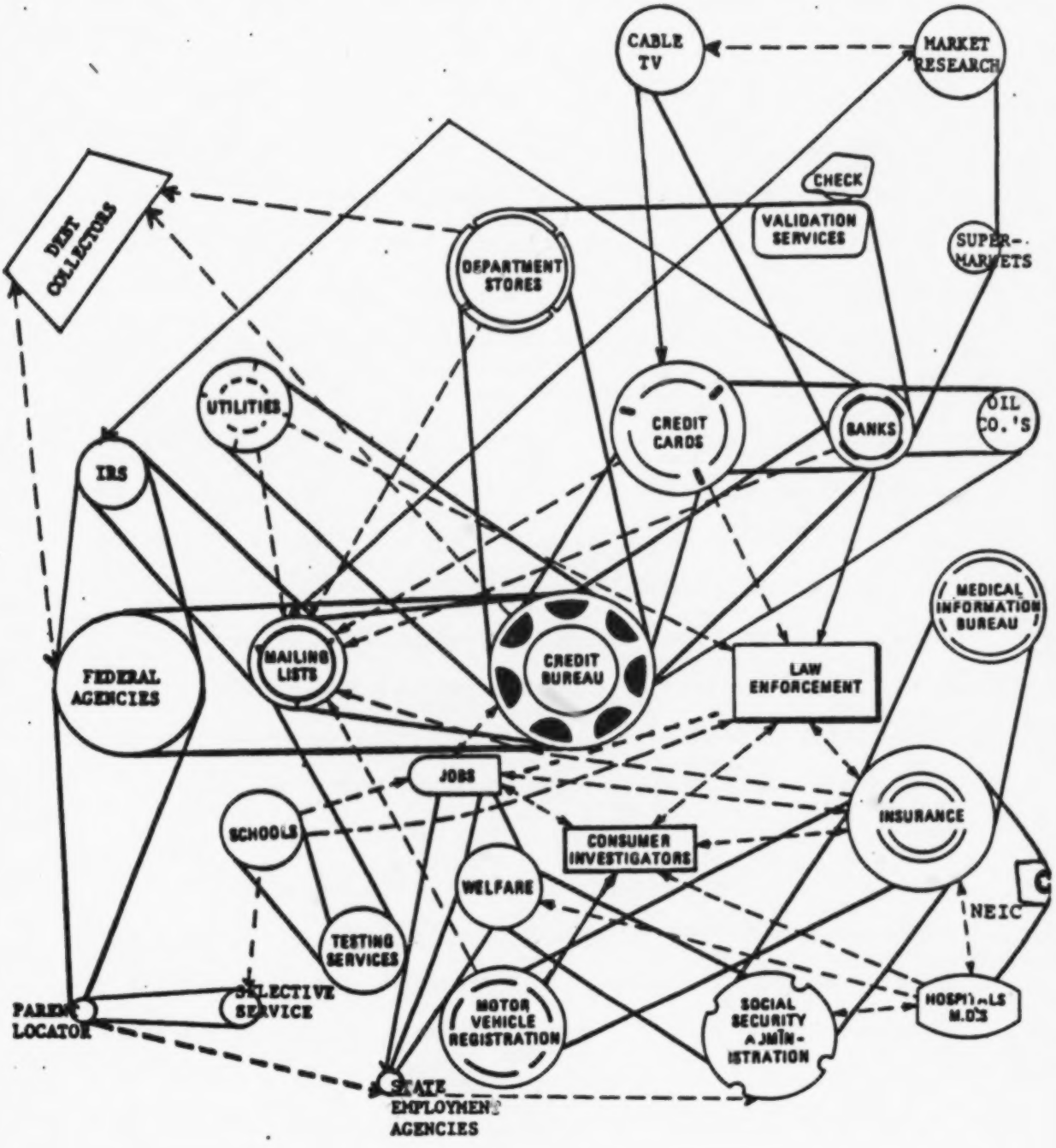
[100]U.S. Congress, Office of Technology Assessment, Federal Government Information Technology: Electronic Record Systems and Individual Privacy, OTA-CIT-296 (Washington, D.C.: U.S. Government Printing Office, June 1986), p. 22.

these new technologies have created legal and policy challenges in information management. Robert Ellis Smith, editor of The Privacy Journal, spoke at the Committee's Ft. Lauderdale public hearing. He noted that the farther the information is from its source, the more likely it is to be incorrect. Exhibit 8-1 is a diagram showing the information sharing among computers. It illustrates how easy it would be to create a composite on an individual from the various pieces of information contained in different computers. Much of the information is of the type that many individuals would consider private, such as income, medical records, and bank records.

New technological advances may lead to improvements in government record keeping, detection and prevention of fraud, waste, and abuse, and law enforcement investigations. At the same time, opportunities for inappropriate, unauthorized, or illegal access to and use of personal information have expanded. Unauthorized access and unauthorized altering of data in one system can easily extend to another linked system. The infection of the Department of Defense's ARPANET System with a virulent computer virus in November 1988 demonstrated a great disadvantage of linking systems together. The sabotage of one system spread to many others and paralyzed more than 6,000 computers in the United States.

For individuals whose names and personal information are filed in a computer that is part of a larger network, the implications are far reaching and are cause for concern. The potential for inappropriate alteration, destruction, disclosure or manipulation of personal information threatens individual privacy. In linked systems, information is exchanged with other organizations without the approval

EXHIBIT 8-1



© 1984 Robert Ellis Smith
(Reprinted with permission of author)

or knowledge of the individual. In other instances, information from one source is combined with that from another, thus creating a profile of the individual to assess his or her eligibility for benefit or entitlement programs. It is also common for data from organizations which regulate their information (such as state and federal government agencies) to be disseminated to others that are not as closely regulated (such as many private organizations). Smith states that this exchange between public and private organizations "obliterates the former clear line between governmental activity and private enterprise, a line that throughout American history has created important constitutional ramifications."[101] For example, Smith says, constitutional limits on unreasonable searches do not include searches conducted by private organizations.[102]

Florida provides on-line access to the state's drivers license file, vehicle registration file, and corporate registration records to customers of a private on-line information provider. Insurance companies, law firms, banks, labor unions, and private investigators have subscribed to the service. The state is preparing to offer the same data to other companies.

Governmental data bases containing personal information began proliferating in the 1970's, and today include: the Social Security Administration, FBI, IRS, states' motor vehicles departments, National Driver Registry, drug abuse data acquisition projects, retail credit

---

[101]Robert Ellis Smith, "The Domino Theory at Work," Privacy Journal, November 1988, p. 5.

[102]Id.

companies, Medical Information Bureau, Tenant Reference Guide, TRW Credit Data, Educational Testing Service, state criminal justice information systems, municipal data systems, Veterans Administration, military, state welfare departments, child abuse projects, and credit card companies.[103]

There is concern that the use of computerized databases, electronic record searches and matches, and computer networking may lead to the creation of a de facto national database containing personal information on most Americans. Use of the social security number as a kind of electronic national identifier facilitates the development of such a database, and at a minimum, may result in the creation of an integrated, general purpose national information system.

The impact of this national data base is magnified because the advanced technologies create the possibility for potential abuse in retrieving, sharing and merging personal information which often goes beyond the original purpose for obtaining the information. New computer and telecommunications applications for processing personal information aid in utilizing information for secondary purposes, such as use of federal employee personal information for locating student loan defaulters, or use of federal tax information for evaluation of a medicaid claim.

Opportunities for individuals to secure employment, insurance, and credit may be put in danger by the misuse of information, as are

---

[103]Robert Ellis Smith, Compilation of State and Federal Privacy Laws, (Washington, D.C.: Privacy Journal, 1988), p. v.

an individual's right to due process and other legal protections.[104]

Kenneth Laudon stated in his book, Dossier Society:

> Contemporary technology can radically alter the organization of power in the United States and with it our traditional conceptions and experience of individual freedom, security, privacy, due process, and, in general, the relationship between individuals and organizations. Fourth generation hardware - microprocessors and computers on a microchip - combined with powerful new concepts in software provide politicians, bureaucrats, and legislators with new tools of governance.[105]

The U.S. Office of Technology Assessment concludes that federal use of new electronic technologies has eroded the protections of the Privacy Act of 1974. Many of the electronic record applications used by federal agencies, such as computer profiling and computer matching, are not explicitly covered by the act or by Office of Management and Budget guidelines.[106] A number of studies have evaluated the implementation and effectiveness of the Privacy Act of 1974. All have concluded that the Act generally has not provided protection for individuals from misuse of personal information by federal agencies.[107] New applications of personal information have undermined the goal of the Privacy Act that individuals be able to control

---

[104] U.S Committee on Government Operations together with Separate Views, Who Cares About Privacy? Oversight of the Privacy Act of 1974 By the Office of Management and Budget and by the Congress, House Report No. 98-455, 98th Congress, 1st Session, (Washington, D.C.: U.S. Government Printing Office, November 1, 1983), p. 1.

[105] Kenneth C. Laudon, Dossier Society, (New York: Columbia University Press, 1986), p. 3.

[106] U.S. Congress, Office of Technology Assessment, Federal Government Information Technology: Electronic Record Systems and Individual Privacy, p. 4.

[107] Id. at 16,17.

information about themselves. In addition, federal agencies have invested only limited time and resources in Privacy Act matters.[108]

A significant problem is the government's collection of non-essential personal information which becomes subject to public disclosure. Some experts believe that individual privacy interests may be best protected by restricting the type of information an agency accumulates and maintains on individuals.[109] In New York, for example, record custodians are required to justify in writing the need for any requested personal information. This recommendation has special relevance for Florida where the Public Records Law makes virtually all types of personal information subject to public disclosure. Florida's liberal Public Records Law also allows such practices as the selling of names and addresses of driver license holders and other lists for purposes of commercial solicitation. Several other states have enacted legislation that prohibits renting or selling of such lists for commercial purposes.

Selling or disclosing video rental lists may also represent an invasion of privacy. Legislation was proposed and enacted in several states to prohibit this practice as a result of the publication of Judge Robert Bork's video rental list. In October 1988, the U.S. Congress passed legislation to prevent video tape rental stores from disclosing information about their customers. The Video Privacy

---

[108]Id. at 25.

[109]Office of Massachusetts Secretary of State, Report of the First National Conference on Issues Concerning Computerized Public Records, Vol. 1, (Boston, Massachusetts: 1986), p. 7.

Protection Act permits a customer to sue in federal court if a video rental or sales outlet discloses which tapes a person borrows or buys, or releases other personally identifiable information. The store may continue to rent lists of customers, provided the individual has an opportunity to prevent such disclosure and the list does not indicate tape titles or descriptions. However, the House killed a provision of the bill that would require library records to be confidential. The FBI argued this provision would interfere with counter-intelligence work, since the agency requires access to information about books and other materials borrowed by library patrons. In Florida, s. 257.261, F.S., protects library registration and circulation records by making them confidential.

Public opinion polls consistently show that Americans are concerned about the issue of personal privacy. About one-half of the American public believes that computers are a threat to privacy, and there is increasing public support for additional activity to protect privacy.[110] There is a need for proper safeguards for personal information given to the government by individuals. The 1988 Compilation of State and Federal Privacy Laws includes more than 650 laws that affect the confidentiality of personal information, and at least 40 of these were enacted during the past year.

Laudon states we now have the choice to determine the impact of information systems on such American values as freedom, security,

---

[110]U.S. Congress, Office of Technology Assessment, Federal Government Information Technology: Electronic Record Systems and Individual Privacy, p. 26.

privacy, and due process.[111] The challenge in Florida is to frame this response in the context of the state's unique Public Records Law. The goals are to provide individuals with protection from unnecessary data collection and to ensure that personal information will not be used, disclosed, or destroyed in inappropriate or harmful ways.

Summary

Concerns exist that a "dossier society" is emerging as both private and public information systems collect and share personal information in ever-increasing amounts. The federal Privacy Act of 1974 places restrictions on the collection, maintenance, use, and dissemination of federal agency records. However, few state laws or policy guidelines govern how personal information is collected and used.

The vast quantities of personal information stored in government computers raise concerns over the ability to protect and balance the privacy of individuals relative to the government's information needs. There is also concern that the use of computerized databases, electronic record searches and matches, and computer networking may lead to the creation of a de facto national database containing personal information about most Americans.

The U.S. Office of Technology Assessment concluded that federal use of new electronic technologies has eroded the protections of the Privacy Act. A significant problem is the government's collection of

---

[111] Kenneth C. Laudon, note 104, supra, p. 5.

non-essential personal information which becomes subject to public disclosure. This fact has special relevance for Florida, where the Public Records Law makes virtually all types of personal information subject to public disclosure.

CHAPTER 9 - RECORDS MANAGEMENT AND ARCHIVAL ISSUES

Background

Records management and archival programs began when documentation was solely in the form of the written word. When paper became the universal recording medium the terms "document" and "paper" became synonomous. Microfilm has become a legal and accepted recording and storage medium mainly because it is eye-readable and is a tamper-proof exact reproduction of the original document. However, the new electronic, magnetic, and optical recording and storage media use digital code. The resulting document can be accessed and reproduced only by machine. The use of these new media create new problems for information and record storage, security, and access. The increased use of microcomputers, electronic mail, and electronic data interchange (EDI), could result in the loss of the historical record because a paper document may not be produced for others to evaluate, store, or protect. The activities of data processing, records management, and information management are rapidly merging, but current policies and procedures governing criteria for the selection, long term retention and preservation of records are inadequate.

Discussion

As was stated in the 1988 report of the New York Special Media Record Project:

> Computers are used to create, process, and store an increasing percentage of the State's public records. Much of the information that state agencies used to store solely on paper, now exists in electronic form on magnetic disks, tapes, and floppy disks. The use of automated systems can bring tremendous benefits to state government because

> information in automated systems is easier to access, manipulate, and disseminate. Yet, the use of computers for record keeping also creates problems for state government. Computers have contributed to an information explosion which has inundated some program managers with more information than they can handle.[112]

Federal, state, and local governments are experiencing difficulty in preserving their documentary records. As noted in the Joint Committee's 1985 Report, Remote Computer Access to Public Records in Florida, our ability to evaluate the historical values of information has not significantly increased, despite the exponential increase in our ability to create, acquire, and store information.

The statutory context for Florida's information and records management activities is composed of three distinct laws. The first of these is the Public Records Law, Chapter 119, F.S. It provides a definition of "public record," establishes the access rights of the public to these records, and defines the responsibilities of record custodians to preserve records and provide access. This law also defines the public agencies subject to its requirements and is noteworthy because it extends to local governments. Chapter 119, Florida Statutes, was one of the first state laws to guarantee public access to public records. The law has been amended numerous times to reflect both changes in technology and in practice. In addition, this law has been heavily litigated and a large body of case law surrounds it.

---

[112]The University of the State of New York, The State Education Department, and State Archives and Records Administration, A Strategic Plan for Managing and Preserving Electronic Records in New York State Government: Final Report of the Special Media Records Project, (Albany: August 9, 1988) p. v.

The second statutory component, s. 257.36, F.S., establishes the Division of Library and Information Services within the Florida Department of State. This statute specifies the duties and authority of the Division with regard to records management and archives programs for state and local agencies. These agencies are statutorily required to designate a records management liaison officer and to "establish and maintain an active and continuing program for the economical and efficient management of records." Section 15.16, F.S., authorizes the Department of State to reproduce records, which records "shall have the same force and effect as the originals thereof."

The third component, requirements for information technology resource planning and management, is statutorily established in Ch. 282, F.S. Both the executive and judicial branches must comply with these requirements which include strategic planning, budget review and security. In addition, s. 282.103, F.S., creates the Suncom network, a telecommunications backbone which is used by state and local agencies for voice, data, video, and facsimile transmissions.

The creation, transmission, storage, and collection of information occurs in the complex legal environment created by these laws. These are not static laws: each of them has been amended to reflect changing technology. New issues continue to emerge which require legislative attention and consideration of further changes.

In Florida, state expenditures for information technology have grown from approximately $150 million in FY 1983-84 to approximately $285 million in FY 1987-88. As a percentage of the state budget, information resources management expenditures have increased from 1.3% in FY 1983-84 to approximately 1.6% in FY 1987-88. The increasing

investment in technology is reflected in an annual growth rate of over 19% in information resources management expenditures.[113]

Data on local government expenditures for information technology are not available from any single source, and it is not possible to determine the extent to which expenditures for information technology are increasing, or, more importantly, the applications which are being developed. The extent to which local governments are cognizant of information management and preservation issues created by the growing use of information technology is also unknown. Although the Bureau of Archives and Records Management, Department of State, provides support to local government, it does not systematically collect data regarding the impact of technology on local government record system policy.

Specific archival problems include the preservation of the software used to process data. Although it is not necessary to include instructions on how to read with every paper document archived, it is necessary that the software used to "read" a data set be available. The rapid obsolescence of software creates a problem in a matter of years while changes in language, such as the change from Middle English to Modern English, took centuries.

In addition to changes in the software used to access, process, and make computer files intelligible, changes in hardware pose threats to the historical record. Without a tape reader, the reels of archived tape are useless. The rapidity of changes in hardware will

---

[113]Florida Information Resource Commission, Annual Report on Information Resources Management, (Tallahassee, Florida: December 1, 1988) p. ii.

require either continual copying of archival records onto new formats capable of being processed by future hardware or retention and maintenance of each type of machine, a difficult if not impossible task.

The physical media on which information is stored also pose threats to the historical record. It is not certain how long magnetic media, such as magnetic tapes, can be stored before they deteriorate. It is clear that temperature, humidity, and light all impact on the useful life of magnetic tape and should be controlled. The physical safety of magnetic and optical media must also be assured, as is the case with paper records.

Records management issues are also changing as information technology is increasingly used by records custodians. Traditional problems of sorting, evaluating, indexing, storing, finding, duplicating, and protecting an organization's records have become even more complex as computers generate vast quantities of data. The advent of photocopying technology also created problems for records managers, but since it was a copy of a document, the difficulties of adjusting to its use were not as great. In addition, the physical media were under the direct control of the records manager.

The use of information technology resources increases the likelihood that the agency or place where the "records" are created is not the same as the one where the records are stored. The location of the stored records may be in another building or even another city. Finding a document requires software that is often created by an organization or individual not under the direct supervision of the manager. As a result, accessing information is no longer a process of

locating a ledger or a file folder, but requires the coordination of many organizations and individuals, from computer operators and programmers to data base managers and input clerks.

Most computer applications are, however, designed to meet the needs of functional requirements of a specific set of users, and do not consider requirements of other elements of the organization. As a result, files which are no longer being used by a system may be periodically purged without regard for future use. The paper trail of a first draft, amendments, annotations, and a final draft may simply disappear. The increasing use by state and local governments of microcomputers adds a new dimension to this problem, because, unlike large data centers, there is generally no systematic "back-up" or copying of computer files by users. Not only may records be lost, the rest of the organization may not know of their existence and cannot assess their importance. Electronic mail will also complicate the responsibilities of records managers. There may be no paper records of communications and, therefore, no documentation will exist.

Summary

Archival and records management programs were developed to deal with paper records. Although microfilm has become a legal and accepted storage medium, the use of electronic, magnetic, and optical storage media create significant new problems for storage, security, and accession. The activities of data processing, records management, and information management are rapidly merging, but there are inadequate policies and procedures governing criteria for selecting

and archiving records, determining if a data base is a public record, or archiving the software used to read records.

Florida is not unique in experiencing difficult issues related to records management in an information age. Federal, state, and local governments are all experiencing significant difficulty in preserving their documentary records.

The creation, transmission, storage, and collection of information occurs in a complex legal environment created by the many statutes governing these activities. These statutes are not static laws: each of them has been amended to reflect the changing environment, specifically technology, and it is clear that new issues will continue to emerge which will require legislative attention and consideration of further changes.

The State of Florida is rapidly adopting information technology for the creation, use, and retention of information. However, the use of technology should not erode our ability to preserve our past nor promote the retention of useless or irrelevant information.

IV. CONCLUSIONS AND RECOMMENDATIONS

Defining Reasonable Access

Based on the findings regarding access to public records, the following conclusions are drawn:

- Electronic records are accessible in many more ways than are manual records, thus making the record custodians' requirement under Ch. 119, F.S., to provide access to records at "reasonable times" and under "reasonable conditions" more difficult to define.
- As more records are automated there is a need to ensure that meaningful and equitable access to them is maintained.

Therefore, it is recommended that:

1) Public record custodians provide access procedures that keep pace with the technology by: providing access to records through automated as well as non-automated means; providing public access terminals on-site once the majority of their records are automated; and allowing the public to use the database management software available so the public may retrieve the desired information more easily. The Legislature should continue to monitor access policies to determine if statutory changes are required.

- Insufficient attention is paid to access requirements when systems are initially designed.

Therefore, it is recommended that:

2) The Information Resource Commission, subject to available resources, develop a rule on systems design and development that addresses public access requirements for state systems.

- Current laws adequately provide for an alternative form of access, remote electronic access, which has been successfully used by several state agencies and local governments.

Therefore, it is recommended that:

3) The law providing for remote electronic access to records should be retained, subject to the Legislative review required by law.

- Current law allows for inconsistencies in fees charged since each record custodian must decide what is "extensive" use of personnel or information technology resources in determining any special charges for copying. These inconsistencies may reflect the variations which exist in each custodian's situation.

Therefore, it is recommended that:

4) Record custodians continue to be provided, under current law, the flexibility of defining what is "extensive" in their situation. However, record custodians should also establish costing algorithms in writing which accurately reflect the costs they incur and form the basis for their charges.

- Some confusion exists as to the responsibilities of centralized data processing departments in maintaining the records of constitutional officers.

Therefore, it is recommended that:

5) The Secretary of State's Division of Library and Information Services review its existing rules on records management to determine whether further clarifications in this area are needed.

Security Concerns

Based on the findings regarding computer security the following conclusions are drawn:

- The automation of public records presents new security problems for record custodians, particularly with the increased networking of computers.

Therefore, it is recommended that:

6) Agencies include in their budgets for new or improved applications the costs associated with providing the necessary security measures for the applications.

- Records security is too often an afterthought, rather than included as a part of the process of automated systems designs.

Therefore, it is recommended that:

7) The Information Resource Commission, subject to available resources, develop a rule requiring agencies to include security considerations as part of each overall systems design project.

- The existing laws and rules regarding the security of records have provided a good framework for the state agencies. However, funding for computer security has been insufficient to meet the agencies' needs.

Therefore, it is recommended that:

8) Increases in state funding for security of state systems be requested. Agencies, particularly those with data centers, should request funds and positions to perform the Information Security Manager function, as mandated by law since 1984.

9) Funds for a disaster recovery facility should be made available to ensure continued operation of critical applications in the event of an emergency. (Legislation to accomplish the latter is included in the Appendices.)

o Those agencies which provide remote electronic access to records under Ch. 119, F.S., are taking steps to ensure the security of those records.

Therefore, it is recommended that:

10) The State continue its current policy of requiring the custodian to ensure the security of the records in a remote electronic access environment and continue to allow the custodian to determine the best method for security in each case.

o The increased use of computerized elections systems intensifies the security concerns for those records, since they are vulnerable to security risks of fraud and error.

Therefore, it is recommended that:

11) The elections laws be amended to:

a) Provide that a manual recount of computerized votes is permissible.

b) Provide authority for the Department of State to develop elections software (as the City of Los Angeles has done) for use by each jurisdiction desiring to do so.

c) Require electronic voting systems to have an audit trail.

d) Require that any vendor which gets approval from the Secretary of State to sell their vote-counting software in Florida must place the source code for their software in escrow.

e) Require the Division of Elections to establish ballot card standards.

f) Require each supervisor of elections to have an independent audit of their system procedures and software performed on a periodic basis.

g) Provide authority for the Department of State to provide technical assistance to local jurisdictions.

It is further recommended that:

12) Increased funding be provided to the Division of Elections to strengthen its ability to certify electronic voting systems and provide better support to supervisors of elections.

13) The Division of Elections:

a) Encourage the phase-out of the use of mechanical lever machines.

b) Strongly encourage, or begin a phasing-in process for, digitizing signatures and bar coding voter I.D. numbers as a way of enhancing the integrity of voting records and speeding up the signature verification process.

c) Require that any vote-counting software used in a Florida election be written in higher-level computer languages, because such languages are easier to analyze for errors or fraud.

d) Encourage the use in Florida elections of public domain software certified by an organization accredited by the National Institute of Standards and Technology. To further that end, the State of Florida, in a consortium with other states, should pursue the possibility of creating an organization of experts to certify the software. The consortium could then be certified by the National Institute.

e) Strongly encourage the use of dedicated computer equipment by the Supervisors of Elections.

(Legislation to accomplish many of these recommendations is included in the Appendices.)

Legal Issues Associated with Optical Storage

Based on the findings concerning the optical storage of documents, the following conclusions are drawn:

- Current law, s. 15.16, F.S., which expressly authorizes the admission of certain records of the Department of State into evidence, does not expressly authorize optically stored documents.

Therefore, it is recommended that:

14) Section 15.16, F.S., be amended to specifically authorize the Department of State to store documents through the use of optical

images and that those records be admissible as evidence in court. (Legislation to accomplish this is included in the Appendices.)

- Except for special cases, current law is silent regarding the use of WORM optical imaging for general archival and evidentiary purposes. This poses problems for custodians who wish to take advantage of the new technology.

Therefore, it is recommended that:

15) The House and Senate Judiciary Committees consider whether a general law is needed to address the use of optically stored documents. Some options for consideration include:

1) Specifically authorizing the admission into evidence of WORM optical images but excluding the admission of erasable ("write many, read many") images.

2) Authorizing the admission into evidence of both erasable and non-erasable optically stored records.

3) Specifically addressing whether paper originals of optically stored documents can be destroyed, and if so, after what period of time.

4) Specifically barring the admission of optically stored records into evidence.

It is further recommended that:

16) The Division of Library and Information Services, Department of State, promulgate rules for state and local agencies regarding the use of optical disk technology.

Dissemination of Public Information

Based on the findings regarding the dissemination of public information, the following conclusions are drawn:

- Florida has no coherent state policy concerning information dissemination by state agencies.

Therefore it is recommended that:

17) The Information Resource Commission address this issue in future State Strategic Plans for Information Resources Management and that agencies be required to include a policy statement on how they disseminate information to the public in their future Strategic Information Resources Management Plans.

- Libraries have historically been instrumental in disseminating information in printed form, and they could likewise be a focal point for the electronic dissemination of information.

Therefore it is recommended that:

18) The Division of Library and Information Services, Department of State, establish an on-line bibliography of public documents and archived documents.

Computer Software Issues

Based on the findings regarding computer software issues, the following conclusions are drawn:

- Some public agencies are copyrighting and selling their software in apparent violation of Chapter 119, F.S., the Public Records

Law. This practice is understandable given the short-term benefits to agencies and jurisdictions of collecting revenue in a time of fiscal constraint. However, when viewed with the long-term perspective of the public's interest, this practice is a threat to the public's ability to know about its government.

- Existing statutes, case law, and attorney general opinions indicate that, except for specific exemptions for certain types of software, most publicly created software is subject to the inspection and copying provisions of Chapter 119, F.S.

Therefore, it is recommended that:

19) The existing law with respect to the inspection and duplication of public records be more stringently enforced by the State Attorneys.

It is further recommended that:

20) The Information Resource Commission, in conjunction with the Department of State and subject to available resources, study the feasibility of establishing a state clearinghouse for software exchange which would serve state and local governments.

- Proprietary software vendors may be reluctant to do business in Florida if contracts do not protect their copyright.

Therefore, it is recommended that:

21) The Division of Purchasing, Department of General Services, examine the existing contract language, specifically Rider 401.14, regarding Protection and Security of Licensed Program Materials, to determine if the standard contract language

concerning the protection of copyrights is sufficient in light of the California court case, BV Engineering v. University of California, Los Angeles, 858 F.2d 1394 (9th Cir. 1988). If it is not sufficient, the Division should revise the language to protect the vendors' copyrights.

Computer Matching

Based on the findings regarding computer matching, the following conclusions are drawn:

- The increased use of computer matching by federal and state agencies raises privacy and other concerns, since few administrative controls, procedures, or guidelines are in place, and currently there is no oversight of computer matching in Florida agencies.
- It is too early to determine whether the federal computer matching legislation, passed in October 1988, will provide the necessary controls for most matching activities conducted in state agencies or if additional state legislation is required to regulate those matching activities not covered under the federal law.

Therefore, it is recommended that:

22) The Joint Committee on Information Technology Resources monitor the implementation of the new federal law and the development of the President's Office of Management and Budget guidelines to determine whether state legislation on computer matching is needed.

Fair Information Practices

Based on the findings regarding fair information practices, the following conclusions are drawn:

- Large amounts of personally identifiable information are stored in state agency computers, and in many cases Florida does not provide statutory protections to assure the accuracy of such information.

Therefore, it is recommended that:

23) A Fair Information Practices Act be implemented in Florida. Such an act should apply only to state agencies and should exempt from its scope various types of information which have proven difficult for other states, such as information on prisoners. (Legislation to accomplish this is included in the Appendices.)

Technological Impacts on Privacy

Based on the findings regarding technological impacts on privacy, the following conclusions are drawn:

- Technological advances have improved government record keeping, detection and prevention of fraud, waste, and abuse, and law enforcement investigations. At the same time, opportunities for inappropriate, unauthorized, or illegal access to and use of personal information have expanded and threaten the privacy of individuals.
- Information law and government policy must respond to the current environment of changing cultural and social circumstances and rapidly developing technologies.

Therefore, it is recommended that:

24) The House and Senate Governmental Operations Committees consider legislation to allow individuals to request that their names and addresses contained in public records as defined in Chapter 119, Florida Statutes, not be released for commercial solicitation purposes.

25) The House and Senate Governmental Operations Committees consider legislation to create a statutory distinction between public records containing personally identifiable information and other public records, and to provide appropriate standards and restrictions for the handling and dissemination of such records.

Records Management and Archives

Based on the findings regarding archival and records management concerns, the following conclusions are drawn:

- The increased use of information technology to create, store, access, and disseminate information has not resulted in increased attention to the preservation of the public record or the increased complexity of records management in an information age.
- There is no evidence that the applications and systems being developed by agencies and local governments are explicity considering archival and dissemination issues, as was recommended in the Joint Committee's 1985 Report, Remote Computer Access to Public Records.

Therefore, it is recommended that:

26) State agencies be required to include records management and archival issues in their Strategic Information Resources

Management Plans and that the Information Resource Commission include these issues in their planning requirements.

27) Criteria be developed by the Information Resource Commission, with the participation of the Division of Library and Information Services, Department of State, and the Information Resources Management Advisory Council, to assure that all new applications adequately address the archival and records management issues.

- o New technologies, including optical storage, electronic data interchange, and electronic mail, pose significant challenges to the state's archival and records management programs. The impact of state and local governments' adoption of these technologies on the public record is not clear.
- o There are no accepted national standards governing this new technology and the issues which concern public sector organizations are different from those of private sector organizations.

Therefore, it is recommended that:

28) The Joint Committee on Information Technology Resources monitor state agencies' use of optical storage, electronic data interchange, electronic mail, and other new technologies to determine if statutorily established archival and records management responsibilities require modification.

29) The Department of State and the Information Resource Commission participate in the standards setting processes of national organizations, such as the American Bar Association and the National Institute of Standards and Technology.

V. REFERENCES

Abdelnour, Charles G. LEGIS - The Legislative Information System. San Diego: City Clerk, 1987.

Allen, Douglas P. "Optical Disk and The Law Texas Style." Inform, April 1988, pp. 43-44.

Associated Press. "Archivists Strive to Save Historic Papers From Crumbling to Dust." Tallahassee Democrat, 5 March 1989, Section A, p. 9.

Becker, Joseph, ed. The Information Society. Volume 5, Number 1. London: Taylor & Francis, 1987.

Betts, Mitch. "Vets Say Optical Disk Will Kill Piles of Paper." Computerworld, 5 September 1988, p. 27.

Bynum, Terrell Ward, ed. Computers & Ethics. Kent, England: Whitstable Litho Ltd., 1985.

Chandler, David. "Computer Virus Usually Not a Terminal Illness, but . . . ." Tallahassee Democrat, Section G, 18 December 1988, pp. 1, 4.

Department of Justice Canada. Access and Privacy: The Steps Ahead. Ottawa: Minister of Supply and Services Canada, 1987.

Division of Statutory Revision of the Joint Legislative Management Committee. Official Florida Statutes. Tallahassee: State of Florida, 1987 and 1988 Supplement.

Dugger, Ronnie. "Annals of Democracy - Counting Votes." The New Yorker, 7 November 1988, pp. 40-108.

ECRI. An Election Administrator's Guide to Computerized Voting Systems. Plymouth Meeting, Pennsylvania: ECRI, November 1988.

Florida Department of Commerce. Florida Facts -- Computer Data Bases. Tallahassee: September 1987.

Florida Department of Highway Safety and Motor Vehicles. Providing Records to the Public, Policy 010. Tallahassee: 15 January 1988.

Florida Department of State. Division of Corporations Public Access User Help Document. Tallahassee: undated.

Florida Information Resource Commission. Annual Report on Information Resources Management. Tallahassee: December 1988.

_____. "Computer Viruses." Florida's IRM Quarterly Review. Vol. 3, No. 1, Tallahassee: January 1989, p. 8.

_____. Draft Report on Contingency Planning for the State's Major Data Centers. Tallahassee: January 1989.

_____. "State of Florida Draft Information Resource Security Standards and Guidelines." Tallahassee: 7 July 1988.

Florida Office of the Attorney General. Florida's Government-In-the-Sunshine and Public Records Law Manual. Volume 10. Tallahassee: First Amendment Foundation, 1988.

Hartog, Curt, and Robert Klepper. "Business Squeeze Pushes Software Sales Up 184%." Computerworld, 22 August 1988, pp. 55-58.

"Hennepin County Legacy Continues." Government Technology. January/February 1989, p. 26.

Hustein, Joseph E. "Executive Briefing - Optical Storage and the Law." Government Technology, November/December 1988, pp. 18-19.

Joint Legislative Committee on Information Technology Resources. Fair Information Practices. Tallahassee: February 1987.

_____. Overview of Computer Security. Tallahassee: January 1984.

_____. Remote Computer Access to Public Records in Florida. Tallahassee: January 1985.

Laudon, Kenneth C. Dossier Society. New York: Columbia University Press, 1986.

Markoff, John. "A Battle To Make Software Free." The New York Times. 11 January 1989, Business Section, pp. 31.

_____. "Computer Experts Say Virus Carried No Hidden Dangers." The New York Times. 9 November 1988, Section A, p. 18, cols. 1-2.

_____. "Networks of Computers At Risk From Invaders." The New York Times. 3 December 1988.

Midford, Robert. "OMB Asks Restraint in Electronic Data." Federal Computer Week, 9 January 1989, pp. 1, 37.

National Association of State Information Systems. Information Systems Technology in State Government. Lexington: 1987.

Office of Management and Budget. "Management of Federal Information Resources." OMB Circular No. A-130. Federal Register. Vol. 50, No. 247, 24 December 1985, pp. 52730-52751.

_____. "Performance of Commercial Activities." OMB Circular No. A-76. Washington D.C.: U.S. Government Printing Office, August 1983.

Office of Massachusetts Secretary of State, Public Records Division. Report of the First National Conference on Issues Concerning Computerized Public Records. 2 vols. Boston: September 1986.

"Optical Disk Law Gunned Down in Texas." Inform, November/December 1988, p. 11.

Park, James R. A Bibliography of the Literature on Optical Storage Technology. NBS Special Publication 500-107. Washington D.C.: U.S. Government Printing Office, December 1983.

Rosenberg, Ronald. "Disasters Waiting to Happen." Tallahassee Democrat, 18 December 1988, Section G, pp. 1, 6.

Ryan, Alan J. "Insurer Samples Optical Disk Transfer." Computerworld, 3 October 1988.

Saltman, Roy. Accuracy, Integrity, and Security in Computerized Vote-Tallying. NBS Special Publication 500-158. Washington D.C.: U.S. Government Printing Office, August 1988.

Savage, J.A. "Data Center Staffers Stung After Saving Tapes for Probe." Computerworld, 31 October 1988, pp. 1, 10.

Schmitt, Richard B. "States May Reproduce Copyright Matter Without Liability, Federal Ruling Holds." The Wall Street Journal, 14 October 1988.

Smith, Robert Ellis. Compilation of State and Federal Privacy Laws. Washington, D.C.: Privacy Journal, 1988.

_____. "The Domino Theory at Work." Privacy Journal, November 1988, p. 5.

"Texas Attorney General Puts a Hold on Official Use of O.D. Storage." Imaging Technology Report, August 1988, pp. 2-3.

U.S. Congress, Office of Technology Assessment. Federal Government Information Technology: Electronic Record Systems and Individual Privacy. OTA-CIT-296. Washington, D.C.: U.S. Government Printing Office, June 1986.

_____. Informing the Nation: Federal Information Dissemination in an Electronic Age. OTA-CIT-396. Washington, D.C.: U.S. Government Printing Office, October 1988.

_____. Science, Technology, and the First Amendment. OTA-CIT-369. Washington, D.C.: U.S. Government Printing Office, January 1988.

U.S. Congressional Record. 14 August 1986, p. S11746.

U.S. Department of Commerce. NTIS Data Base Services and Federal Technology in Machine-Readable Formats. Springfield, Virginia: 1983.

_____. NTIS Software Products. Springfield, Virginia: 1984.

U.S. General Accounting Office. Computer Matching: Assessing Its Costs and Benefits. GAO/PEMD-87-2. Washington, D.C.: U.S. Government Printing Office, November 1986.

_____. Computer Matching: Factors Influencing the Agency Decisionmaking Process. GAO/PEMD-87-3BR. Washington, D.C.: U.S. Government Printing Office, November 1986.

_____. Privacy Act: Federal Agencies' Implementation Can Be Improved. GAO/GGD-86-107. Washington, D.C.: U.S. Government Printing Office, August 1986.

"U.S. Government Agency Continues Efforts To Define Legal Acceptability of Optical Disk Record." EDPACS- The EDP Audit Control Security Newsletter, May 1988, p. 13.

U.S. House of Representatives, Committee on Government Operations. Computer Matching and Privacy Protection Act of 1987 - Hearing on S. 496. 100th Congress, 1st Session, Washington, D.C.: 23 June 1987.

_____. Computer Matching and Privacy Protection Act of 1988. 100th Congress, 2nd Session, Report 100-802. Washington, D.C.: U.S. Government Printing Office, 27 July 1988.

_____. Computer Security Act of 1987. Report 100-153, Part 2, 100th Congress, 1st Session, Washington, D.C.: 11 June 1987.

_____. Electronic Collection and Dissemination of Information by Federal Agencies: A Policy Overview. House Report 99-560, 99th Congress, 2nd Session, Washington, D.C.: U.S. Government Printing Office, 29 April 1986.

_____. Who Cares About Privacy? Oversight of the Privacy Act of 1974 by the Office of Management and Budget and by the Congress. House Report No. 98-455, 98th Congress, 1st Session. Washington, D.C.: U.S. Government Printing Office, 1 November 1983.

The University of the State of New York, The State Education Department, and State Archives and Records Administration. A Strategic Plan For Managing and Preserving Electronic Records in New York State Government: Final Report of The Special Media Records Project. Albany: August 1988.

"Utah DataShare Online." Government Technology. January/February 1989, p. 4.

Will, George. "Two-tier Drug Culture is Emerging." Tallahassee Democrat. 8 January 1989.

Williams, Robert F., ed. Legality of Optical Storage -- Admissibility in Evidence of Optically Stored Records. Chicago: Cohasset Associates, Inc., 1987.

Williams, Roxanne. "Getting the Word Out." Government Data Systems. June/July 1985, pp. 28-29.

"You Can't Fight City Hall, But You Can Access It." Tallahassee Democrat, 22 February 1989.

APPENDICES

SB 498

By Senators Stuart, Johnson and Gardner

A bill to be entitled

An act relating to information resources; creating the Information System Disaster Recovery Act; providing legislative findings and intent; providing definitions; providing for a disaster recovery facility to be administered by the Department of General Services; providing requirements for such facility; providing that certain procedures and test results of the facility are exempt from public record disclosure requirements; requiring future legislative review of such exemptions pursuant to the Open Government Sunset Review Act; requiring departments to perform certain tests; authorizing political subdivisions of the state to contract with the disaster recovery facility for disaster recovery services; creating the Disaster Recovery Facility Advisory Council; providing for membership, staff support, and meetings of the council; creating the Florida Information System Disaster Recovery Trust Fund; providing for funding and administering the fund; providing appropriations; providing an effective date.

WHEREAS, the state provides essential governmental services through the use of advanced information systems, and

WHEREAS, the provision of some of these critical services is not possible without automated support, and

This publication was produced at l erage cost of 2 cents per page for the information of members of the Legislature and the public.

CODING: Words stricken are deletions; words underlined are additions.

WHEREAS, in order to ensure the continuity and reliability of critical state information systems, a means of providing backup and recovery capabilities is required, NOW, THEREFORE,

Be It Enacted by the Legislature of the State of Florida:

Section 1. Short title.--This act may be cited as the "Information System Disaster Recovery Act."

Section 2. Findings and intent.--

(1) The Legislature finds and declares that many state programs are critically dependent upon automated information systems; that the loss of these information systems would present a real and immediate danger to public health, safety, and welfare; and that a continuing effort is needed to ensure a reliable and secure means of recovering from any disaster affecting data and information processing facilities used by state agencies. It is the intent of the Legislature that the head of each department which provides critical public services through the use of automated information systems ensure the continuation of such services in the event of a disaster which affects the primary processing center supporting delivery of such services. It is further the intent of the Legislature that the Information Resource Commission ensure that adequate policies and procedures assist and facilitate the continuation of critical services to the public and to state agencies in the event of a disaster which affects a primary processing facility.

(2) The Legislature also finds and declares that disaster recovery for information systems is most economically and effectively provided through coordinated statewide

CODING: Words stricken are deletions; words underlined are additions.

strategies that meet the needs of individual departments. It is the intent of the Legislature that the head of each department participate in and support the statewide information system disaster recovery strategies prescribed in this act.

Section 3. Definitions.--As used in this act, the term:

(1) "Agency" means those entities described in chapter 216, Florida Statutes.

(2) "Application" means a separately identifiable and interrelated set of information technology resources and communications, as determined by each agency, that is used to support an agency objective.

(3) "Commission" means the Information Resource Commission as created by section 282.304, Florida States.

(4) "Data" means a representation of information that is stored, communicated, interpreted, or processed by automated means.

(5) "Department" means the principal administrative unit within the executive branch of state government as defined in chapter 20, Florida Statutes. For the purposes of this act, the State Board of Administration, the Executive Office of the Governor, and the Game and Fresh Water Fish Commission shall be considered departments.

(6) "Disaster" means a condition in which data is unavailable as a result of a natural or manmade occurrence that is of sufficient duration to cause significant disruption in the accomplishment of agency program objectives, as determined by agency management.

CODING: Words stricken are deletions; words underlined are additions.

(7) "Executive administrator" means the executive administrator of the Information Resource Commission as provided in section 282.304, Florida Statutes.

(8) "Information technology resources" means data processing hardware and software and services, supplies, personnel, facility resources, maintenance, and training. The commission shall determine, by rule, the process control devices to be excluded from this definition.

(9) "Primary processing facility" means the information technology resources used to regularly provide production services for an application. A primary processing facility may include a central computer room, telecommunications support resources, environmental protection equipment, power systems, central processing units, data transmission and storage resources, peripheral equipment, supplies, personnel, data, systems and application software, and input and output devices.

(10) "Production services" means the usual and scheduled operation of information technology resources in support of an application.

Section 4. Disaster recovery facility.--

(1) The Department of General Services shall provide a disaster recovery facility to serve any agency that is dependent upon information technology resources for the delivery of essential services. The Department of General Services shall establish procedures for reviewing agency needs and develop a disaster recovery facility in consultation with the commission. The Department of General Services shall acquire, by lease or purchase, the disaster recovery facility and shall contract with a facility manager for the operation of the facility. The Department of General Services may

CODING: Words stricken are deletions; words underlined are additions.

establish prequalification and bonding requirements, commensurate with the responsibility and nature of the services to be provided, for any contract entered into under this act. The disaster recovery facility may include a central computer room, telecommunications support resources, environmental protection equipment, power systems, central processing units, data transmission and storage resources, peripheral equipment, supplies, personnel, data, systems and application software, and input and output devices.

(2) The commission shall establish criteria for applications affecting the executive branch which are to be supported by the disaster recovery facility and the Supreme Court and the Legislature may establish criteria for applications affecting the judicial and legislative branches, respectively, which are to be supported by the disaster recovery facility.

(3) Communications services provided to the disaster recovery facility shall be integrated with the SUNCOM Network to provide the greatest possible efficiency and effectiveness in recovery of computer network operations.

(4) The disaster recovery facility shall provide production services for critical applications of an agency if a primary processing facility is unable to perform its mission due to a disaster, prepare for recovery from such a disaster, and test recovery capability. In addition, the facility may perform processing tasks for testing and developing application systems for state agencies. Other than when required by an actual emergency affecting a primary processing facility, the disaster recovery facility may not be used to provide routine production services for any agency.

CODING: Words stricken are deletions; words underlined are additions.

(5) Operating procedures, testing schedules, and the results of tests performed by the disaster recovery facility are confidential and exempt from disclosure under chapters 119 and 286, Florida Statutes, however, the Auditor General shall have access to such information in the performance of his duties. This exemption is subject to the Open Government Sunset Review Act in accordance with section 119.14, Florida Statutes.

(6) Each department served by the disaster recovery facility shall test its ability to recover critical processing services at least annually.

(7) Political subdivisions of the state may contract with the disaster recovery facility for information system backup and disaster recovery services. In case of a conflict between the needs of an agency or a department and the needs of a political subdivision of the state for critical processing services, the disaster recovery facility shall give first priority to the agency or department.

(8) By October 1 of each year, beginning October 1, 1992, the Department of General Services shall report to the executive administrator on tests conducted by the disaster recovery facility and the facility's capability to provide essential services provided by a primary processing facility if such facility is unable to perform its mission due to a disaster. Such reports shall be confidential and exempt from disclosure under chapters 119 and 286, Florida Statutes, however, the Auditor General shall have access to such information in the performance of his duties. This exemption is subject to the Open Government Sunset Review Act in accordance with section 119.14, Florida Statutes.

CODING: Words stricken are deletions; words underlined are additions.

Section 5. Disaster Recovery Facility Advisory Council.--

(1)(a) There is created the Disaster Recovery Facility Advisory Council to advise the Department of General Services regarding any matter relating to the operation and management of the disaster recovery facility. The information security managers of each department served by the disaster recovery facility shall be members of the council. The executive administrator and the director of the Division of Communications of the Department of General Services shall be ex officio members of the council.

(b) The council shall annually elect a chairman from among its members. The Department of General Services shall provide the necessary staff support for the council. The council shall meet at least biannually upon the call of the chairman.

Section 6. Florida Information System Disaster Recovery Trust Fund; funding.--

(1) There is created the Florida Information System Disaster Recovery Trust Fund for the purpose of financing the disaster recovery facility as provided by this act. The Department of General Services shall administer the trust fund.

(2) The moneys in the trust fund shall consist of moneys appropriated by the Legislature and shall be paid by each agency, and each agency shall include in its budget estimates its pro rata share of the costs as determined by the Department of General Services. Moneys paid by political subdivisions of the state that contract with the disaster recovery facility for information system backup and disaster

recovery services shall be used to offset the costs borne by each agency.

Section 7. (1) The sum of $300,000 is hereby appropriated from the General Revenue Fund to the Information Resource Commission to coordinate the development of disaster recovery plans for each department, where applicable. Such funds may be used for term contracts for services, software licenses, and planning and startup expenses necessary to carry out the provisions of this act.

(2) The sum of $50,000 is hereby appropriated from the General Revenue Fund to the Department of General Services to be used for planning and startup expenses necessary to carry out the provisions of this act.

Section 8. This act shall take effect July 1, 1989, or upon becoming a law, whichever occurs later.

****

SENATE SUMMARY

Creates the Information System Disaster Recovery Act. Requires the Department of General Services to establish a disaster recovery facility to provide support services for agencies and departments in the event of a disaster which affects information processing facilities. Requires communications services provided to the disaster recovery facility to be integrated with the SUNCOM Network. Provides that the operating procedures, testing schedules, and the results of tests performed by the facility are exempt from public disclosure requirements. Requires departments that are serviced by the facility to perform certain annual tests. Authorizes political subdivisions of the state to contract with the facility for disaster recovery services. Requires the Department of General Services to provide certain annual reports concerning the facility's capabilities. Creates the Disaster Recovery Facility Advisory Council to advise the Department of General Services on the operation and management of the disaster recovery facility. Creates the Florida Information System Disaster Recovery Trust Fund. Provides appropriations.

CODING: Words stricken are deletions; words underlined are additions.

SB 499

By Senators Stuart, W.D. Childers, Johnson, Gardner and Brown

This publication was produced at average cost of 2 cents per page for the information of members of the Legislature and the public.

A bill to be entitled

An act relating to elections; amending s. 97.012, F.S.; providing duties of the Secretary of State; amending s. 97.021, F.S.; providing definitions; creating s. 101.015, F.S.; requiring the Department of State to adopt rules; amending s. 101.292, F.S.; revising the definition of the term "voting equipment"; amending s. 101.294, F.S.; requiring the department to review certain contracts relating to the purchase of voting equipment; authorizing the department to negotiate certain agreements and contracts relating to the purchase of voting systems by local governments; amending s. 101.31, F.S.; providing for experimental use of voting systems; amending s. 101.5603, F.S.; providing definitions; amending s. 101.5605, F.S.; providing for additional testing of a voting system by the department; amending s. 101.5606, F.S.; providing an additional requirement for the approval of voting systems by the department; amending s. 101.5607, F.S.; requiring a supervisor of elections to file voting system software with the department; authorizing the department to review county voting systems; authorizing the department to prepare software for voting systems; amending s. 101.5609, F.S.; requiring the department to adopt standards for certain ballots; creating s. 101.591, F.S.; requiring the department to

CODING: Words stricken are deletions; words underlined are additions.

audit county voting systems; amending s. 102.166, F.S.; providing requirements for elections canvassing boards; providing procedures for manual recounts by such boards; creating the Bureau of Voting Systems Certification within the Division of Elections of the department; providing an appropriation; providing an effective date.

Be It Enacted by the Legislature of the State of Florida:

Section 1. This act shall be known as the "Voter Protection Act."

Section 2. Subsection (5) is added to section 97.012, Florida Statutes, to read:

97.012 Secretary of State as chief election officer.--The Secretary of State is the chief election officer of the state, and it is his responsibility to:

(5) Provide technical assistance to the supervisors of elections on voting systems.

Section 3. Present subsection (26) of section 97.021, Florida Statutes, is renumbered as subsection (27), and a new subsection (26) is added to said section to read:

97.021 Definitions.--The following words and phrases when used in this code shall be construed as follows:

(26) "Voting system" means a method of casting and processing votes that functions wholly or partly by use of mechanical, electromechanical, or electronic apparatus or by use of paper ballots and includes, but is not limited to, the procedures for casting and processing votes and the programs,

CODING: Words stricken are deletions; words underlined are additions.

operating manuals, tabulating cards, printouts, and other software necessary for the system's operation.

Section 4. Section 101.015, Florida Statutes, is created to read:

101.015 Department of State to adopt rules.--

(1) The Department of State shall adopt rules which establish minimum standards for hardware and software for voting systems. Such rules shall contain standards for:

(a) Functional requirements;

(b) Performance levels;

(c) Physical and design characteristics;

(d) Documentation requirements; and

(e) Evaluation criteria.

(2) Each odd-numbered year the Department of State shall review the rules governing standards and certification of voting systems to determine the adequacy and effectiveness of such rules in assuring that elections are fair and impartial.

(3) The Department of State shall adopt rules to achieve and maintain the maximum degree of correctness, impartiality, and efficiency of the procedures of voting, including write-in voting, and of counting, tabulating, and recording votes by voting systems used in this state.

(4)(a) The Department of State shall adopt rules establishing minimum security standards for voting systems.

(b) Each supervisor of elections shall establish written procedures to assure accuracy and security in his county, and such procedures shall be reviewed in each odd-numbered year by the Department of State.

(c) Each supervisor of elections shall submit any revisions to the security procedures to the Department of

CODING: Words stricken are deletions; words underlined are additions.

State at least 45 days before the first election in which they are to take effect.

(5) All voting systems purchased on or after January 1, 1990, must meet the minimum standards established under subsection (1). All voting systems in use on or after July 1, 1993, must meet the minimum standards established under subsection (1).

Section 5. Subsection (2) of section 101.292, Florida Statutes, is amended to read:

101.292 Definitions.--As used in ss. 101.292-101.295, the following terms shall have the following meanings:

(2) "Voting equipment" means new or used voting machines and materials, parts, or other equipment necessary for the maintenance or improvement of voting machines, the individual or combined retail value of which is in excess of $1,000. The term "voting equipment" also includes electronic or electromechanical voting systems, voting devices, and automatic tabulating equipment as defined in s. 101.5603, as well as <u>ballot cards,</u> materials, parts, or other equipment necessary for the operation and maintenance of such systems and devices.

Section 6. Subsection (1) of section 101.294, Florida Statutes, is amended, and subsection (4) is added to said section to read:

101.294 Purchase and sale of voting equipment.--

(1) The Division of Elections of the Department of State shall adopt uniform rules for the purchase, use, and sale of voting equipment in the state. No governing body shall purchase or cause to be purchased any voting equipment unless such equipment has been certified for use in this state

CODING: Words stricken are deletions; words <u>underlined</u> are additions.

by the Department of State and the purchase contract has been reviewed by the Department of State.

(4) The Department of State may, with the assistance of the Division of Purchasing of the Department of General Services, negotiate and execute purchasing agreements and contracts under which any governing body may purchase any element of a voting system.

Section 7. Section 101.31, Florida Statutes, is amended to read:

101.31 Experimental use of voting systems machines.--The board of county commissioners of any county, or the governing body of any municipality, may provide for experimental use of any voting system machine-or-machines at any election in one or more precincts. The use of any voting system machine-or-machines on an experimental basis shall be valid for all purposes.

Section 8. Present subsection (7) of section 101.5603, Florida Statutes, is renumbered as subsection (8) and a new subsection (7) is added to said section to read:

101.5603 Definitions.--As used in this act, the term:

(7) "Software" means the programs and routines used to employ and control the capabilities of data processing hardware, including, without limitation, operating systems, compilers, assemblers, utilities, library routines, maintenance routines, applications, and computer networking programs.

Section 9. Paragraph (a) of subsection (2) of section 101.5605, Florida Statutes, is amended to read:

101.5605 Examination and approval of equipment.--

(2)(a) Any person owning or interested in an electronic or electromechanical voting system may submit it to

CODING: Words stricken are deletions; words underlined are additions.

the Department of State for examination. The vote counting segment shall be certified after a satisfactory evaluation testing has been performed according to electronic industry standards. This testing shall include, but is not limited to, testing of all software required for the system's operation ~~the basic source program and its security;~~ the ballot reader; the vote processor, especially in its logic and memory components; the digital printer; the fail-safe operations; the counting center environmental requirements; and the equipment reliability estimate. For the purpose of assisting in examining the system, the department shall employ or contract for services of at least one individual who is expert in one or more fields of data processing, mechanical engineering, and public administration and shall require from him a written report of his examination.

Section 10. Subsection (12) is added to section 101.5606, Florida Statutes, to read:

101.5606 Requirements for approval of systems.--No electronic or electromechanical voting system shall be approved by the Department of State unless it is so constructed that:

(12) It is capable of providing records from which the operation of the voting system may be audited.

Section 11. Section 101.5607, Florida Statutes, is amended to read:

(Substantial rewording of section. See s. 101.5607, F.S., for present text.)

101.5607 Department of State to maintain voting system information; prepare software.--

(1)(a) Copies of the program codes and the user and operator manuals and copies of all software and any other

CODING: Words ~~stricken~~ are deletions; words underlined are additions.

information, specifications, or documentation required by the Department of State relating to an approved electronic or electromechanical voting system and its equipment must be filed with the Department of State by the supervisor of elections at the time of purchase or implementation. Any such information or materials that are not on file with and approved by the Department of State, including any updated or modified materials, may not be used in an election.

(b) Within 24 hours after the completion of any logic and accuracy test conducted pursuant to s. 101.5612(1), the supervisor of elections shall send by certified mail to the Department of State a copy of the tabulation program which was used in the logic and accuracy testing.

(c) The Department of State may, at any time, review the voting system of any county to ensure compliance with the Electronic Voting Systems Act.

(d) Section 119.07(3)(r) applies to all software on file with the Department of State.

(2)(a) The Department of State may develop software for use with an electronic or electromechanical voting system. The standards and examination procedures developed for software apply to all software developed by the Department of State.

(b) Software prepared by the Department of State is a public record pursuant to chapter 119 and shall be provided at the actual cost of duplication.

Section 12. Subsection (8) is added to section 101.5609, Florida Statutes, to read:

101.5609 Ballot requirements.--

(8) The Department of State shall adopt rules prescribing standards for ballots used in electronic or

CODING: Words stricken are deletions; words underlined are additions.

electromechanical voting systems. Such standards shall ensure that ballots are counted in a uniform and consistent manner and shall include, without limitation, standards for the:

(a) Physical characteristics of ballots;

(b) Physical characteristics of ink for ballots;

(c) Printing of ballots; and

(d) Scoring of ballots.

Section 13. Section 101.591, Florida Statutes, is created to read:

101.591 Voting system audit.--

(1) The Department of State shall audit, at least every 5 years, the voting system in each county. Within 30 days after completing the audit, the Department of State shall furnish a copy of the audit to the supervisor of elections and the board of county commissioners.

(2) The audit shall consist of a study and evaluation of the voting system used during any primary, general, municipal, or presidential preference primary election to provide reasonable assurance that the system is properly controlled, can accurately count votes, provides adequate safeguards against unauthorized manipulation and fraud, and complies with the requirements of law and rules of the Department of State.

Section 14. Section 102.166, Florida Statutes, is amended to read:

102.166 Protest of election returns; procedure; venue.--

(1) Any candidate for nomination or election, or any elector qualified to vote in the election related to such candidacy, shall have the right to protest the returns of the

CODING: Words stricken are deletions; words underlined are additions.

election as being erroneous by filing with the appropriate canvassing board a sworn, written protest.

~~(2)(a)~~ Such protest shall be filed with the canvassing board prior to the time the canvassing board adjourns or within 5 days after of midnight of the date the election is held, whichever last occurs.

~~(b)--Before-canvassing-such-returns-the-canvassing board-shall-examine-the-counters-on-the-machines-or-the tabulation-of-the-paper-ballots-cast-in-such-precincts-and determine-whether-the-returns-correctly-reflect-the-votes cast;--if-there-is-a-discrepancy-between-the-returns-and-the counters-of-the-machines-or-the-tabulation-of-the-paper ballots-cast;-the-counters-of-such-machines-or-the-precinct tabulation-of-the-paper-ballots-cast-shall-be-presumed correct;-and-such-votes-shall-be-canvassed-accordingly;--The rights-of-all-parties-in-interest-to-appeal-to-the-court-for protection-against-error-are-not-annulled;~~

(3) Before canvassing the returns of the election, the canvassing board shall:

(a) When paper ballots are used, examine the tabulation of the paper ballots cast.

(b) When voting machines are used, examine the counters on the machines of nonprinter machines or the printer-pac on printer machines. If there is a discrepancy between the returns and the counters of the machines or the printer-pac, the counters of such machines or the printer-pac shall be presumed correct.

(c) When electronic or electromechanical equipment is used, the canvassing board shall examine precinct records and election returns. If there is a clerical error, such error shall be corrected by the county canvassing board. If there

CODING: Words stricken are deletions; words underlined are additions.

is a discrepancy which could affect the outcome of an election, the canvassing board may recount the ballots on the automatic tabulating equipment.

(4)(a) Any candidate whose name appeared on the ballot, any political committee that supports or opposes an issue which appeared on the ballot, or any political party whose candidates' names appeared on the ballot may file a written request with the county canvassing board for a manual recount.

(b) Such request must be filed with the canvassing board prior to the time the canvassing board adjourns or within 5 days after midnight of the date the election was held, whichever occurs later.

(c) The county canvassing board may authorize a manual recount. If a manual recount is authorized, the county canvassing board must notify each candidate whose race is being recounted of the time and place of such recount.

(d) The manual recount must include at least three precincts and at least 1 percent of the total votes cast for such candidate or issue. The person who requested the recount shall choose three precincts to be recounted, and, if other precincts are recounted, the county canvassing board shall select the additional precincts.

(5) If the manual recount indicates an error in the vote tabulation which could affect the outcome of the election, the county canvassing board shall:

(a) Recount the remaining precincts with the vote tabulation system;

(b) Request the Department of State to verify the tabulation software; or

(c) Manually recount all ballots.

CODING: Words stricken are deletions; words underlined are additions.

(6) Any manual recount shall be open to the public.

(7) Procedures for a manual recount are as follows:

(a) A counting team of at least two electors shall be appointed by the county canvassing board to count no more than 1,200 ballots. A counting team must have, when possible, members of at least two political parties.

(b) If a counting team is unable to determine a voter's intent in casting a ballot, the ballot shall be presented to the county canvassing board for it to determine the voter's intent.

(8) If the county canvassing board determines the need to verify the tabulation software, the county canvassing board shall request in writing that the Department of State verify the software.

(9) When the Department of State verifies such software, the department shall:

(a) Compare the software used to tabulate the votes with the software filed with the Department of State pursuant to s. 101.5607; and

(b) Check the election parameters.

(10) The Department of State shall respond to the county canvassing board within 3 working days.

(11)(9) Any candidate for nomination or election, or any elector qualified to vote in the election related to such candidacy, shall have the right to protest the returns of the election or the practices attendant thereto as being fraudulent by presenting to any circuit judge of the circuit wherein such fraud is alleged to have occurred a sworn, written protest. If it is alleged that fraudulent returns or practices exist in more than one county, venue for such

CODING: Words stricken are deletions; words underlined are additions.

protest shall be in any such county wherein such fraud is alleged to have occurred.

(a) The protest shall be presented to a circuit judge prior to the time the canvassing board adjourns or within 5 days after of midnight of the date the election occurs, whichever last occurs.

(b) The circuit judge to whom the protest is presented shall have authority to fashion such orders as he may deem necessary to insure that such allegation is investigated, examined, or checked; to prevent or correct such fraud; or to provide any relief appropriate under such circumstances. Any candidate or elector presenting such a protest to a circuit judge shall be entitled to an immediate hearing thereon or to any appropriate relief.

Section 15. (1) There is created a Bureau of Voting Systems Certification within the Division of Elections of the Department of State which shall provide technical support to the supervisors of elections and which is responsible for voting system standards and certification. The positions necessary for the bureau to accomplish its duties shall be established through the budgetary process.

(2) Sixteen initial positions are established in the bureau, and the sum of $669,000 is hereby appropriated to the Division of Elections from the General Revenue Fund for the purpose of carrying out the provisions of this act.

Section 16. This act shall take effect January 1, 1990, except that this section and section 15 shall take effect July 1, 1989, or upon this act becoming a law, whichever occurs later.

CODING: Words stricken are deletions; words underlined are additions.

****

SENATE SUMMARY

Creates the Voter Protection Act to revise provisions of the Florida Election Code relating to the operation of voting systems by local governments. Requires the Department of State to adopt rules which establish hardware and software standards for voting systems. Requires the department to review a local government's purchase contracts for voting equipment. Authorizes the department to negotiate and execute purchasing agreements for such contracts. Requires that voting systems be capable of producing audit records. Requires a supervisor of elections to file certain information relating to a voting system and its equipment with the department.. Requires the department to adopt standards for ballots used in voting systems. Requires the department to audit each county's voting system no less than every 5 years. Revises the requirements for canvassing the returns of an election. Provides requirements for a manual recount. Creates the Bureau of Voting Systems Certification within the Division of Elections of the Department of State.

CODING: Words stricken are deletions; words underlined are additions.

SB 444

By Senators Stuart, Johnson and Gardner

A bill to be entitled

An act relating to the Department of State; amending s. 15.16, F.S.; providing for optical image record storage; prescribing admissibility and authenticity of records so stored; providing for receipt of certain records through facsimile or other electronic transfer; providing for certification and electronic transmittal of department records; authorizing the department to adopt rules; providing an effective date.

Be It Enacted by the Legislature of the State of Florida:

Section 1. Section 15.16, Florida Statutes, is amended to read:

15.16 Reproduction of records; admissibility in evidence; electronic receipt and transmission of records; certification.--

(1) The Department of State may cause to be made copies of any records maintained by it by miniature photographic microfilming or microphotographic processes or any other photographic, mechanical, or other process heretofore or hereafter devised, including electronic data processing.

(2) Photographs, nonerasable optical images, or microphotographs in the form of film, facsimiles, or prints of any records made in compliance with the provisions of this section shall have the same force and effect as the originals thereof, and shall be treated as originals for the purpose of their admissibility in evidence. Duly certified or

This publication was produced at an average cost of 2 cents per page for the information of members of the Legislature and the public.

CODING: Words stricken are deletions; words underlined are additions.

authenticated reproductions of such photographs, nonerasable optical images, or microphotographs shall be admitted in evidence equally with the original photographs, nonerasable optical images, or microphotographs.

(3) The Department of State may cause to be received electronically any records that are required to be filed with it pursuant to chapter 607, chapter 608, chapter 617, chapter 620, or chapter 621, through facsimile or other electronic transfers, for the purpose of filing such records. The originals of all such electronically transmitted records must be executed in the manner provided by law and must contain in the lower left-hand corner of the first page the name, address, and telephone number of the preparer of the original and, if prepared by an attorney licensed in this state, the preparer's Florida Bar membership number. The receipt of such electronic transfer constitutes delivery to the department as required by law.

(4) The department may certify and electronically transmit any record maintained by it. The certification must be evidenced by a certification code on each page transmitted which must include the document's charter or filing number, date of transmission, and page number of the total number of pages transmitted, and a sequential certification number assigned by the department which will identify the transmission and be available for verification of any transmitted certified document.

(5) If not otherwise provided by law, the Department of State shall determine, by rule, the appropriate format for, number of copies of, manner of execution of, method of electronic transmission of, and amount of and method of

CODING: Words stricken are deletions; words underlined are additions.

payment of fees for any document placed under its jurisdiction for filing or recordation.

Section 2. This act shall take effect upon becoming a law.

****

SENATE SUMMARY

Provides that nonerasable optical images of records required to be filed with the Department of State have the same force and effect as the original records. Authorizes the department to receive, electronically through facsimile or other medium, records that must be filed with it pursuant to chs. 607, 608, 617, 620, and 621, F.S. Authorizes the department to certify and electronically transmit any record in its possession. Prescribes information that must be included in records electronically received or transmitted. Authorizes the department to adopt rules with respect to electronic receipt and transmission of records.

CODING: Words stricken are deletions; words underlined are additions.

By Senators Stuart, Johnson and Gardner

SB 483

A bill to be entitled

An act relating to public records; creating the "Florida Fair Information Practices Act"; providing purpose and intent; providing exemptions; providing definitions; providing for departmental reports of the existence, type, and disclosures of certain public records containing personal information; requiring copies of such reports be maintained for public use; providing for notice to certain persons concerning the collection, maintenance, and use of personal information; providing procedures for requesting a change in personal information in certain public records; requiring the Division of Library and Information Services of the Department of State to recommend rules of procedure; requiring the Administration Commission to adopt rules to implement this act; providing for an annual report to the Legislature; providing an appropriation; providing severability; providing effective dates.

Be It Enacted by the Legislature of the State of Florida:

Section 1. Short title.--This act may be cited as the "Florida Fair Information Practices Act."

Section 2. Legislative intent; construction; application.--

(1) The purpose of this act is to enhance the rights of individuals about whom personal information is collected by

This publication was produced at an ... age cost of 2 cents per page for the information of members of the Legislature and the public.

departments, and to require that departments which collect or maintain personal information that is subject to public disclosure:

(a) Ensure the accuracy of such information in cooperation with the individuals who are the subjects of the information; and

(b) Periodically report on certain interdepartmental data transfers of personal information subject to public disclosure.

(2) This act shall be liberally construed to assist individuals in identifying:

(a) Personal information about them that is a public record and subject to public disclosure;

(b) The purpose for which such personal information is collected, maintained, and used by a department; and

(c) Whether personal information that is subject to public disclosure is accurate and complete.

(3) This act does not create any substantive rights for any individual; any substantive or procedural rights for a prisoner, as defined in section 944.02(5), Florida Statutes, or for persons under the supervision of the Department of Corrections; or any property or liberty interests subject to the protection of the United States Constitution.

(4) This act does not apply to personal information contained in public records maintained in the State University System or in the Florida State Archives by the Division of Library and Information Services of the Department of State.

(5) This act does not apply to personal information contained in the following types of public records:

(a) A telephone book or directory which is used exclusively for telephone and directory information;

CODING: Words stricken are deletions; words underlined are additions.

(b) Any card catalog, book, or other resource material in any library;

(c) Any compilation of information containing only names and addresses which is used exclusively for the purpose of mailing department information;

(d) Letters of inquiry or comment about department programs, requests for general information, and responses to such letters and requests;

(e) Employee travel files and patient medical records and medical claims records of state employees, former employees, and eligible dependents pursuant to section 110.123(9), Florida Statutes;

(f) Telephone messages and logs of a department; or

(g) Any automated or manual record maintained by the Department of Corrections on any individual currently or formerly under the custody, control, or supervision of the Department of Corrections.

(6) This act does not apply to personal information obtained during civil or criminal litigation or adversarial administrative proceedings or in anticipation of imminent civil or criminal litigation or adversarial administrative proceedings.

(7) This act does not apply to contractors, consultants, or vendors from whom a department purchases goods or services.

Section 3. Definitions.--For purposes of this act:

(1) "Department" means the principal administrative unit within the executive branch of state government, and includes the Executive Office of the Governor.

(2) "Individual" means a natural person.

CODING: Words stricken are deletions; words underlined are additions.

(3) "Personal information" means any data maintained by a department that pertains to an individual and which, because of name, identifying number, mark, or description, may be readily associated with a particular individual. The term includes, but is not limited to, the individal's name; social security number; physical description; home address; home telephone number; financial information; and educational, medical, or employment history.

(4) "System of records" means one or more records pertaining to one or more individuals which is maintained by a department for a particular purpose or function and from which personal information may be retrieved using the name of an individual or an identifying number, symbol, or other identifying item assigned to an individual.

Section 4. Report required; annual report; copies for public use.--

(1) Each department that maintains a system of records that contains personal information which is subject to public disclosure shall provide a report, for the previous fiscal year, on the existence and type of such personal information that it maintains. Such reports shall be provided to the Department of State, by October 1 of each year, for publication in the next available issue of the Florida Administrative Weekly. For each system of records which contains personal information subject to public disclosure, such reports must include the following:

(a) The name of the department and the name of the principal unit within the department and the title and business address of the custodian responsible for maintaining the records;

(b) A brief description, including the categories of individuals about whom personal information is maintained, the estimated number of individuals in each category at the end of each fiscal year, and the type of personal information maintained for each category of individuals;

(c) The anticipated internal use by the department of the personal information;

(d) Other agencies of the executive branch, judicial branch, or any political subdivision of the state which regularly receive personal information from the department, listed by the type of personal information disclosed;

(e) Other agencies of the executive branch, judicial branch, or any political subdivision of the state which have been provided on-line computer access to the personal information maintained by the department;

(f) Other departments which received data file transfers from the department of personal information concerning 1,000 or more individuals at any one time during the preceding year, including the categories of individuals in the transfer and the estimated number of individuals in each category. Departments may not divide such data file transfers to avoid the requirements of this paragraph; and

(g) A citation to the legal authority, by statute or rule, and a general description of the policies and practices of the department regarding methods for collecting, maintaining, retrieving, sharing, and disposing of personal information.

(2) In addition, each report must specify the department procedures whereby an individual, at his request, can find out if the department maintains personal information relating to him that is subject to public disclosure; can gain

CODING: Words stricken are deletions; words underlined are additions.

access to such personal information; and can contest its accuracy or completeness.

(3) Each department shall maintain, for public use, copies of the reports required in this section.

Section 5. Notice that personal information is a public record.--

(1) When a department requests personal information directly from the individual who is the subject of the personal information, and that personal information is, at the time it is requested, subject to public disclosure, the department shall provide to that individual an oral or written notice at the time of the request, which notice contains:

(a) The name and address of the department requesting the information;

(b) A citation to the legal authority, by statute or rule, under which the department requests the personal information;

(c) A statement as to whether the individual is required to supply the personal information;

(d) The consequences to the individual, if any, of not providing all or any part of the requested personal information;

(e) A statement of anticipated uses of the personal information by the department, including, but not limited to, disclosures to other agencies of the executive branch, judicial branch, or any political subdivision of the state and the internal uses of the information by the department; and

(f) The fact that the personal information will be subject to public disclosure.

CODING: Words stricken are deletions; words underlined are additions.

(2) The methods by which the department may provide written notice of the facts required in subsection (1) include, but are not limited to:

(a) A statement on the form used to request the personal information;

(b) A statement on a separate sheet provided with the form used to request the personal information;

(c) A statement in a pamphlet, booklet, manual, or other printed matter provided to the individual at the time the personal information is requested; or

(d) A sign or notice prominently posted so that it can be easily observed and read by individuals at the time personal information is requested from them.

(3) This section does not apply to a request for personal information:

(a) If the request is made by a law enforcement officer, as defined in section 111.065, Florida Statutes, in the performance of his duties; or

(b) If the request is made by a department of its employees.

Section 6. Requests to change personal information in public records.--

(1) An individual who is the subject of personal information that is maintained by a department and is subject to public disclosure may contest the accuracy or completeness of the personal information. To do so, the individual must make a written request to the department that maintains the personal information. The request must include:

(a) A statement of disagreement containing a description of the contested personal information;

CODING: Words stricken are deletions; words unde lined are additions.

(b) The changes necessary to make the personal information accurate or complete; and

(c) The individual's name and the address where the department may contact him.

(2) Within 30 days after receiving an individual's written request, the department may request verification from the individual seeking to change personal information.

(3) Within 30 days after receiving an individual's written request and any verification to change personal information, the department shall review the request and:

(a) Change the personal information according to the request and notify the individual in writing; or

(b) Deny the request and notify the individual, in writing, of the reasons for the decision and the name, title, and business address of the official who denied the request.

(4) If an individual's request has been denied, he may provide to the department a concise written statement which sets forth his reasons for disagreeing with the department's decision.

(5) The department shall maintain the statement of disagreement and the department's decision to deny the request. The department shall make, in all public records that contain disputed personal information, a clear notation that indicates which portions are in dispute.

(6) This section does not supersede or provide an additional remedy to any existing statutory procedures or administrative rules for correcting personal information in public records.

(7) This section does not apply to criminal intelligence or criminal investigative records; department

CODING: Words stricken are deletions; words underlined are additions.

personnel or retirement system records; or records of applicants for employment in departments.

Section 7. Rules.--

(1) The Division of Library and Information Services of the Department of State shall prepare and submit to the Administration Commission recommendations for rules of procedure to implement this act. The rules shall specify procedures that a department must use to comply with this act and shall include model language for use in meeting the reporting and notification requirements established in sections 4 and 5.

(2) The Administration Commission shall review, and revise if necessary, the rules recommended by the division and shall adopt rules of procedure to implement this act.

Section 8. Annual report.--The Division of Library and Information Services of the Department of State shall provide a report to the Legislature on the implementation of this act by February 1, 1990, and annually thereafter by February 1. The report shall include, but not be limited to:

(1) A summarized description of the annual department reports required by section 4;

(2) The estimated cost of implementing this act;

(3) The estimated number of individuals who contest the accuracy or completeness of personal information in public records;

(4) The number of hearings held pursuant to chapter 120, Florida Statutes, as a result of this act;

(5) Discussions of any problems encountered in implementing this act; and

(6) Recommendations for further action by the Legislature.

CODING: Words stricken are deletions; words underlined are additions.

Section 9. This act does not give any individual a cause of action for damages or authorize the institution of any civil proceeding against a department or its employee for refusal to comply with an individual's request to change personal information.

Section 10. The sum of $32,331 is hereby appropriated from the General Revenue Fund to the Department of State for the purposes of administering this act during fiscal year 1989-1990.

Section 11. Severability.--If any provision of this act or the application thereof to any person or circumstance is held invalid, the invalidity shall not affect other provisions or applications of the act which can be given effect without the invalid provision or application, and to this end the provisions of this act are declared severable.

Section 12. This act shall take effect January 1, 1990, except that this section and section 7 shall take effect upon becoming a law.

CODING: Words stricken are deletions; words underlined are additions.

****

SENATE SUMMARY

Creates the "Florida Fair Information Practices Act." States that the Legislature intends this act to enhance the rights of individuals about whom personal information is collected by executive agencies of this state and to require agencies that collect personal information that is subject to public disclosure to ensure the accuracy of that information and to periodically report on interdepartmental transfers of such information. Exempts certain personal information from the act. Requires each department that maintains a system of records that contains personal information to submit to the Department of State, for publication in the Florida Administrative Weekly, an annual report on the existence and type of information that it maintains, how it intends to use the information, with what other agencies it has shared the information, how an individual can find out what information subject to public disclosure the department maintains about him, and how that individual can contest the accuracy of the information. Requires a department to maintain copies of those reports for public use. Provides that a department which requests from an individual personal information that is subject to disclosure must tell him whether he is required to give the information, how it will be used, and that it is subject to public disclosure. Provides procedures for requesting a change in personal information in certain public records. Requires the Division of Library and Information Services of the Department of State to recommend rules of procedure to implement this act, and requires the Administration Commission to review, revise as necessary, and adopt such rules. Provides for an annual report to the Legislature. Provides severability.

CODING: Words stricken are deletions; words underlined are additions.

APPENDIX A

PROPOSED LEGISLATION

SB 483

By Senators Stuart, Johnson and Gardner

A bill to be entitled

An act relating to public records; creating the "Florida Fair Information Practices Act"; providing purpose and intent; providing exemptions; providing definitions; providing for departmental reports of the existence, type, and disclosures of certain public records containing personal information; requiring copies of such reports be maintained for public use; providing for notice to certain persons concerning the collection, maintenance, and use of personal information; providing procedures for requesting a change in personal information in certain public records; requiring the Division of Library and Information Services of the Department of State to recommend rules of procedure; requiring the Administration Commission to adopt rules to implement this act; providing for an annual report to the Legislature; providing an appropriation; providing severability; providing effective dates.

Be It Enacted by the Legislature of the State of Florida:

Section 1. Short title.--This act may be cited as the "Florida Fair Information Practices Act."

Section 2. Legislative intent; construction; application.--

(1) The purpose of this act is to enhance the rights of individuals about whom personal information is collected by

This publication was produced at an ... age cost of 2 cents per page for the information of members of the Legislature and the public.

CODING: Words stricken are deletions; words underlined are additions.

departments, and to require that departments which collect or maintain personal information that is subject to public disclosure:

(a) Ensure the accuracy of such information in cooperation with the individuals who are the subjects of the information; and

(b) Periodically report on certain interdepartmental data transfers of personal information subject to public disclosure.

(2) This act shall be liberally construed to assist individuals in identifying:

(a) Personal information about them that is a public record and subject to public disclosure;

(b) The purpose for which such personal information is collected, maintained, and used by a department; and

(c) Whether personal information that is subject to public disclosure is accurate and complete.

(3) This act does not create any substantive rights for any individual; any substantive or procedural rights for a prisoner, as defined in section 944.02(5), Florida Statutes, or for persons under the supervision of the Department of Corrections; or any property or liberty interests subject to the protection of the United States Constitution.

(4) This act does not apply to personal information contained in public records maintained in the State University System or in the Florida State Archives by the Division of Library and Information Services of the Department of State.

(5) This act does not apply to personal information contained in the following types of public records:

(a) A telephone book or directory which is used exclusively for telephone and directory information;

CODING: Words stricken are deletions; words underlined are additions.

(b) Any card catalog, book, or other resource material in any library;

(c) Any compilation of information containing only names and addresses which is used exclusively for the purpose of mailing department information;

(d) Letters of inquiry or comment about department programs, requests for general information, and responses to such letters and requests;

(e) Employee travel files and patient medical records and medical claims records of state employees, former employees, and eligible dependents pursuant to section 110.123(9), Florida Statutes;

(f) Telephone messages and logs of a department; or

(g) Any automated or manual record maintained by the Department of Corrections on any individual currently or formerly under the custody, control or supervision of the Department of Corrections.

(6) This act does not apply to personal information obtained during civil or criminal litigation or adversarial administrative proceedings or in anticipation of imminent civil or criminal litigation or adversarial administrative proceedings.

(7) This act does not apply to contractors, consultants, or vendors from whom a department purchases goods or services.

Section 3. Definitions.--For purposes of this act:

(1) "Department" means the principal administrative unit within the executive branch of state government, and includes the Executive Office of the Governor.

(2) "Individual" means a natural person.

CODING: Words stricken are deletions; words underlined are additions.

(3) "Personal information" means any data maintained by a department that pertains to an individual and which, because of name, identifying number, mark, or description, may be readily associated with a particular individual. The term includes, but is not limited to, the individal's name; social security number; physical description; home address; home telephone number; financial information; and educational, medical, or employment history.

(4) "System of records" means one or more records pertaining to one or more individuals which is maintained by a department for a particular purpose or function and from which personal information may be retrieved using the name of an individual or an identifying number, symbol, or other identifying item assigned to an individual.

Section 4. Report required; annual report; copies for public use.--

(1) Each department that maintains a system of records that contains personal information which is subject to public disclosure shall provide a report, for the previous fiscal year, on the existence and type of such personal information that it maintains. Such reports shall be provided to the Department of State, by October 1 of each year, for publication in the next available issue of the Florida Administrative Weekly. For each system of records which contains personal information subject to public disclosure, such reports must include the following:

(a) The name of the department and the name of the principal unit within the department and the title and business address of the custodian responsible for maintaining the records;

CODING: Words ~~stricken~~ are deletions; words underlined are additions.

(b) A brief description, including the categories of individuals about whom personal information is maintained, the estimated number of individuals in each category at the end of each fiscal year, and the type of personal information maintained for each category of individuals;

(c) The anticipated internal use by the department of the personal information;

(d) Other agencies of the executive branch, judicial branch, or any political subdivision of the state which regularly receive personal information from the department, listed by the type of personal information disclosed;

(e) Other agencies of the executive branch, judicial branch, or any political subdivision of the state which have been provided on-line computer access to the personal information maintained by the department;

(f) Other departments which received data file transfers from the department of personal information concerning 1,000 or more individuals at any one time during the preceding year, including the categories of individuals in the transfer and the estimated number of individuals in each category. Departments may not divide such data file transfers to avoid the requirements of this paragraph; and

(g) A citation to the legal authority, by statute or rule, and a general description of the policies and practices of the department regarding methods for collecting, maintaining, retrieving, sharing, and disposing of personal information.

(2) In addition, each report must specify the department procedures whereby an individual, at his request, can find out if the department maintains personal information relating to him that is subject to public disclosure; can gain

CODING: Words stricken are deletions; words underlined are additions.

access to such personal information; and can contest its accuracy or completeness.

(3) Each department shall maintain, for public use, copies of the reports required in this section.

Section 5. Notice that personal information is a public record.--

(1) When a department requests personal information directly from the individual who is the subject of the personal information, and that personal information is, at the time it is requested, subject to public disclosure, the department shall provide to that individual an oral or written notice at the time of the request, which notice contains:

(a) The name and address of the department requesting the information;

(b) A citation to the legal authority, by statute or rule, under which the department requests the personal information;

(c) A statement as to whether the individual is required to supply the personal information;

(d) The consequences to the individual, if any, of not providing all or any part of the requested personal information;

(e) A statement of anticipated uses of the personal information by the department, including, but not limited to, disclosures to other agencies of the executive branch, judicial branch, or any political subdivision of the state and the internal uses of the information by the department; and

(f) The fact that the personal information will be subject to public disclosure.

CODING: Words stricken are deletions; words underlined are additions.

(2) The methods by which the department may provide written notice of the facts required in subsection (1) include, but are not limited to:

(a) A statement on the form used to request the personal information;

(b) A statement on a separate sheet provided with the form used to request the personal information;

(c) A statement in a pamphlet, booklet, manual, or other printed matter provided to the individual at the time the personal information is requested; or

(d) A sign or notice prominently posted so that it can be easily observed and read by individuals at the time personal information is requested from them.

(3) This section does not apply to a request for personal information:

(a) If the request is made by a law enforcement officer, as defined in section 111.065, Florida Statutes, in the performance of his duties; or

(b) If the request is made by a department of its employees.

Section 6. Requests to change personal information in public records.--

(1) An individual who is the subject of personal information that is maintained by a department and is subject to public disclosure may contest the accuracy or completeness of the personal information. To do so, the individual must make a written request to the department that maintains the personal information. The request must include:

(a) A statement of disagreement containing a description of the contested personal information;

CODING: Words stricken are deletions; words underlined are additions.

(b) The changes necessary to make the personal information accurate or complete; and

(c) The individual's name and the address where the department may contact him.

(2) Within 30 days after receiving an individual's written request, the department may request verification from the individual seeking to change personal information.

(3) Within 30 days after receiving an individual's written request and any verification to change personal information, the department shall review the request and:

(a) Change the personal information according to the request and notify the individual in writing; or

(b) Deny the request and notify the individual, in writing, of the reasons for the decision and the name, title, and business address of the official who denied the request.

(4) If an individual's request has been denied, he may provide to the department a concise written statement which sets forth his reasons for disagreeing with the department's decision.

(5) The department shall maintain the statement of disagreement and the department's decision to deny the request. The department shall make, in all public records that contain disputed personal information, a clear notation that indicates which portions are in dispute.

(6) This section does not supersede or provide an additional remedy to any existing statutory procedures or administrative rules for correcting personal information in public records.

(7) This section does not apply to criminal intelligence or criminal investigative records; department

CODING: Words stricken are deletions; words underlined are additions.

personnel or retirement system records; or records of applicants for employment in departments.

Section 7. Rules.--

(1) The Division of Library and Information Services of the Department of State shall prepare and submit to the Administration Commission recommendations for rules of procedure to implement this act. The rules shall specify procedures that a department must use to comply with this act and shall include model language for use in meeting the reporting and notification requirements established in sections 4 and 5.

(2) The Administration Commission shall review, and revise if necessary, the rules recommended by the division and shall adopt rules of procedure to implement this act.

Section 8. Annual report.--The Division of Library and Information Services of the Department of State shall provide a report to the Legislature on the implementation of this act by February 1, 1990, and annually thereafter by February 1. The report shall include, but not be limited to:

(1) A summarized description of the annual department reports required by section 4;

(2) The estimated cost of implementing this act;

(3) The estimated number of individuals who contest the accuracy or completeness of personal information in public records;

(4) The number of hearings held pursuant to chapter 120, Florida Statutes, as a result of this act;

(5) Discussions of any problems encountered in implementing this act; and

(6) Recommendations for further action by the Legislature.

CODING: Words stricken are deletions; words underlined are additions.

Section 9. This act does not give any individual a cause of action for damages or authorize the institution of any civil proceeding against a department or its employee for refusal to comply with an individual's request to change personal information.

Section 10. The sum of $32,331 is hereby appropriated from the General Revenue Fund to the Department of State for the purposes of administering this act during fiscal year 1989-1990.

Section 11. Severability.--If any provision of this act or the application thereof to any person or circumstance is held invalid, the invalidity shall not affect other provisions or applications of the act which can be given effect without the invalid provision or application, and to this end the provisions of this act are declared severable.

Section 12. This act shall take effect January 1, 1990, except that this section and section 7 shall take effect upon becoming a law.

CODING: Words stricken are deletions; words underlined are additions.

****

SENATE SUMMARY

Creates the "Florida Fair Information Practices Act." States that the Legislature intends this act to enhance the rights of individuals about whom personal information is collected by executive agencies of this state and to require agencies that collect personal information that is subject to public disclosure to ensure the accuracy of that information and to periodically report on interdepartmental transfers of such information. Exempts certain personal information from the act. Requires each department that maintains a system of records that contains personal information to submit to the Department of State, for publication in the Florida Administrative Weekly, an annual report on the existence and type of information that it maintains, how it intends to use the information, with what other agencies it has shared the information, how an individual can find out what information subject to public disclosure the department maintains about him, and how that individual can contest the accuracy of the information. Requires a department to maintain copies of those reports for public use. Provides that a department which requests from an individual personal information that is subject to disclosure must tell him whether he is required to give the information, how it will be used, and that it is subject to public disclosure. Provides procedures for requesting a change in personal information in certain public records. Requires the Division of Library and Information Services of the Department of State to recommend rules of procedure to implement this act, and requires the Administration Commission to review, revise as necessary, and adopt such rules. Provides for an annual report to the Legislature. Provides severability.

CODING: Words ~~stricken~~ are deletions; words <u>underlined</u> are additions.

APPENDIX B

MAILED QUESTIONAIRES

JOHN W. VOGT
President

JON MILLS
Speaker

THE FLORIDA LEGISLATURE

JOINT COMMITTEE ON INFORMATION TECHNOLOGY RESOURCES

Senator George Stuart, Jr., Chair
Representative Anne Mackenzie, Vice-Chair

EDWIN A. LEVINE, STAFF DIRECTOR
805, First Florida Bank Building
215 South Monroe Street
Tallahassee, Florida 32301
Telephone (904) 488-4646

August 11, 1988

Dear Record Custodian:

Enclosed is a survey designed to examine the practices of record custodians with respect to the provision of public access to computer-stored public records. The survey is part of an interim study by the Joint Legislative Committee on Information Technology on the issue of electronic collection and dissemination of information by state and local governments.

This study is a continuation of the Committee's activities in this area, which began in 1984 by examining remote access to public records. The results of the survey will be used to develop an agenda of issues for a proposed series of public hearings to be held in early 1989 and to develop draft legislation, if necessary, for the 1989 legislative session.

In order to solicit the input of as wide a variety of record custodians as possible with respect to these issues, we are sending the survey to: 1) state information resource managers; 2) a sample of city and county managers; and 3) county constitutional officers. Information about your experiences with computer-stored records is critical to our evaluation of the issue; therefore, we would appreciate the return of the completed survey by September 15 in the enclosed business reply envelope.

Thank you for your time in completing the survey and if you have any questions, please do not hesitate to call committee staff at (904) 488-4646 (Suncom 278-4646).

Sincerely,

Geo Stuart Jr.

George Stuart, Jr.
Chairman

Enclosure

APPENDIX B-1

The Florida Legislature
Information Technology Resources Committee
805 First Florida Bank Building
215 S. Monroe Street
Tallahassee, Florida 32301
(904)488-4646 (Suncom) 278-4646

Name: _____

Title: _____

Agency -- City/County: _____

	n	%
State =	94	31%
County=	192	64%
City =	16	5%

Please return in the enclosed business reply envelope by September 15, 1988

ACCESS TO AUTOMATED PUBLIC RECORDS

Please circle your response for each of the following questions. In some cases, you may choose more than one response.

1. What portion of your agency's records are computerized? (Please estimate)

		n	%
a.	None	30	10
b.	Some, but less than 25%	40	13
c.	Between 25-50%	59	20
d.	Between 50-75%	53	18
e.	More than 75%	117	39
	no response	3	1
		302	101 (due to rounding)

(If you answered "<u>none</u>", skip to Question #26)

2. Does your agency have any written internal policy(ies) regarding how public access is provided to computer-stored public records?

		n	%	
a.	Yes	60	23	(Excludes those without
b.	No	205	77	automation & not responding)
		265	100	

If <u>yes</u>, please describe below or attach copy.

53 of 60, or 88%, of those with written policies attached copies.

3. How does your agency currrently provide access (as required by Chapter 119, Florida Statutes) for the inspection/examination (as opposed to duplication) of computer-stored public records? (Circle all that apply)

Total n = 267

		n	%
a.	Via computer terminal (on site)	138	52
b.	Original record	133	50
c.	Photocopy	132	49
d.	Microfilm/microfiche	127	48
e.	Computer printout	210	79
f.	Other _____	22	8

4. In what physical form(s) do you provide the public with copies of computer-stored public records? (Circle all that apply)

Total n = 266

		n	%
a.	Photocopy	181	68
b.	Computer tape or diskette	111	42
c.	Microfilm/microfiche	94	35
d.	Computer printout	223	84
e.	Other _____	12	5

5. Do you charge for providing copies of computer-stored public records?

		n	%
a.	Yes	195	74
b.	No	62	24
	Depends	6	2
		263	100

(Excludes those not responding)

(If you answered 'no', skip to Question #10.)

6. How much do you charge for providing copies of computer-stored information? (Please circle appropriate letter(s) and also indicate charges.)

Total n = 197

		Charges n	Charges %
a.	Charge per unit of records (e.g. per page, sheet of microfiche)	136	69
b.	Charge per record (e.g. 10¢ per name)	62	32
c.	Charge by computer time (e.g. $100 per hour)	63	32
d.	Subscription fee	9	5
e.	Other _____	58	29

APPENDIX B-1

7. Do the charges you assess for the copies recover all of the costs of providing the copies?

		n	%
a.	Yes	100	51
b.	No	96	49
	Depends	2	1
		198	101 (due to rounding)

8. Do you have a formal charging system based on a cost collection/cost allocation model for determining the costs to be charged for copies?

		n	%
a.	Yes	40	21
b.	No	155	80
		195	101 (due to rounding)

If yes, please provide a copy with your response to this survey.

9. What cost factor(s) are recovered by your charges? (Circle all that apply) Total n = 191

		n	%
a.	Labor	97	51
b.	Computer peripheral equipment use	66	35
c.	Utilities	25	13
d.	Computer time	103	54
e.	Duplication media (e.g. paper, tape, microfiche)	158	83
f.	Other _____	17	9

10. Has your agency installed any database management software in its computer system?

		n	%
a.	Yes	136	53
b.	No	120	47
		256	100

If yes, please list by name.

_____

_____

11. Are you having any specific problems meeting requests for computer access to public records?

		n	%
a.	Yes	32	12
b.	No	234	88
		266	100

If yes, please describe.

29 of 32, or 91% of those experiencing problems described them.

12. Are any requests ever made to the record custodian for copies of large portions of computerized data bases containing public records?

		n	%
a.	Yes	131	49
b.	No	135	51
		266	100

(If your answer is no, skip to Question #15.)

13. How often are these requests made?

		n	%
a.	4 or more times a month	41	31
b.	1-3 times a month	35	26
c.	Less than once a month	57	43
		133	100

14. How do you fulfill such requests?

		n	%
a.	Provide the requested information on computer tape or diskette(s)	30	22
b.	Provide printout of data base	28	21
c.	Unable to meet request	3	2
d.	Other (Usually a combination of the above methods)	74	55
		135	100

Please cite any problems you may have in providing data base copies (e.g., providing daily updates).

35 responses to this question

15. Do you ever receive requests for copies of computer programs (software) written by agency personnel?

		n	%
a.	I never receive requests for copies of computer programs (software) written by agency personnel.	132	51
b.	I receive requests for copies of agency programs (software) written by agency personnel, but I do not provide copies.	9	3
c.	I receive requests for copies of agency programs (software) and I provide the copies.	67	26
d.	My agency does not utilize computer programs (software) written by agency personnel.	53	20
		261	100

16. Has your agency copyrighted any software which was written by agency personnel?

		n	%
a.	Yes	9	4
b.	No	248	96
		257	100

17. Has your agency ever exchanged any software, which was written by agency personnel, with another public agency?

		n	%
a.	Yes	101	39
b.	No	156	61
		257	100

18. Has your agency ever sold any of its software which was written by agency personnel?

		n	%
a.	Yes	14	5
b.	No	244	95
		258	100

If yes, please provide the following information:

Sold To	Selling Price	Price was greater than the cost of duplication (Yes or No)
11 responses to this question.		

19. Has your agency entered into any agreements or contracts with the private sector for them to market your agency-produced software?

		n	%
a.	Yes	7	3
b.	No	251	97
		258	100

For the purposes of Questions 20-24, two kinds of computer access to public records are defined as follows:

<u>Dial-up Access</u> - is provided by the connection of a user's personal computer, terminal or workstation to an agency computer via the user's telephone and a modem (equipment that converts computer code into telephone signals).

<u>Dedicated-line Access</u> - is provided by the installation of a telecommunications line from the user's personal computer, terminal, or workstation to the agency computer.

---

20. What type(s) of electronic access exists between your agency computer and private- sector users?

		n	%
a.	Dial-up	25	10
b.	Dedicated line	14	5
c.	Both (a) & (b)	7	3
d.	Neither	211	82
		257	100

(If you answered "<u>Neither</u>", skip to Question #22)

21. Who initiated the electronic access?

		n	%
a.	Record custodian	9	18
b.	Users	10	20
c.	Combination of (a) & (b)	20	40
d.	Other	11	22
		50	100

22. What type(s) of electronic access between your agency computer and private sector users have you considered providing, but which does not yet exist?

		n	%
a.	Dial-up facilities	32	13
b.	Dedicated lines	17	7
c.	Both (a) & (b)	22	9
d.	Neither	173	71
		244	100

23. Has your agency entered into any agreements or contracts with the private sector for them to market the electronic access to your agency's public records?

		n	%
a.	Yes	7	3
b.	No	248	97
		255	100

APPENDIX B-1

24. What is your general assessment of the feasibility of providing electronic access to computer-stored public records?

200 responded to this question. The majority did not consider it feasible due to security and cost concerns.

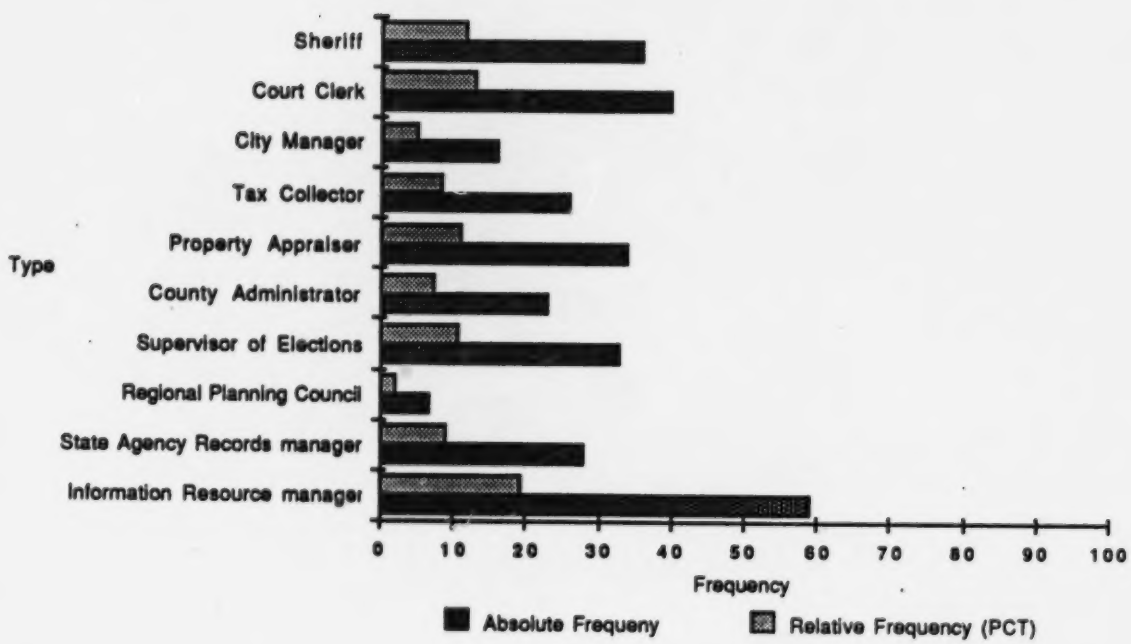
25. Would you be interested in testifying before or providing written comments to the Joint Committee on Information Technology Resources on the effect of Florida's Public Records Law on access to and distribution of publicly-created software?

		n	%
a.	Yes	53	21
b.	No	202	79
		255	100

26. Please feel free to provide any additional comments concerning the impact of automation on the public's ability to access public records and the record custodian's ability to provide access.

69 responded to this opportunity.

Survey Response Rate by Respondent Type



APPENDIX B-1A

JOHN W. VOGT
President

JON MILLS
Speaker

THE FLORIDA LEGISLATURE
JOINT COMMITTEE ON
INFORMATION TECHNOLOGY RESOURCES

Senator George Stuart, Jr., Chair
Representative Anne Mackenzie, Vice-Chair

EDWIN A. LEVINE, STAFF DIRECTOR
805, First Florida Bank Building
215 South Monroe Street
Tallahassee, Florida 32301
Telephone (904) 488-4646

October 25, 1988

MEMORANDUM

TO: Information Resource Managers

FROM: Ed Levine EL

SUBJECT: Survey of Computer Matching Activities in State Departments

---

The issues related to computer matching activities have resulted in the recent passage of the Computer Matching and Privacy Protection Act of 1988 by the U.S. Senate and House. The President signed the bill into law on October 18, 1988, and it has become Public Law 100-503. This bill establishes procedures to regulate the use of computer matching carried out by federal agencies or by other agencies using federal records subject to the Privacy Act of 1974. I have enclosed a copy of the bill and a brief analysis. You may want to order the two reports of the U.S. House Committee on Government Operations on this issue:

1. Report on the Hearing Before a Subcommittee of the Committee on Government Operations on the Computer Matching and Privacy Protection Act of 1987 (S. 496), June 23, 1987.

2. Report on Computer Matching and Privacy Protection Act of 1988 (H.R. 4699), July 27, 1988.

There is also a great deal of computer matching occurring at the state level, where states match records with other state agencies, federal and local agencies, and with organizations in the private sector, such as banks. A preliminary assessment of computer matching in Florida state departments last year indicated that millions of records were being matched annually. In order to assess the current situation regarding computer matching in Florida, Joint Committee staff are conducting a follow-up to last year's preliminary survey. I would appreciate your responses to as many items as possible on the survey with respect to your organization (e.g., division, bureau, etc.). If there are any other organizational units in your agency which should receive this form, please duplicate it in its entirety

and forward it to the appropriate individual(s) for completion. Also, please attach to your questionnaire a list of the people to whom a duplicate questionnaire was sent. I would appreciate your assistance in returning all survey forms completed by your agency to this office by **Monday, November 21.**

On a related issue, Joint Committee staff are redrafting the Fair Information Practices legislation for our chairman to introduce during the 1989 session. Using the new federal law as a guide, this draft may include several provisions which would affect computer matching in state agencies. I would appreciate any comments you may have on the enclosed Federal Computer Matching and Privacy Protection Act.

I will provide you with a copy of the staff report on computer matching and the draft FIPA legislation when they are available. If you have any questions, please call me or Sharon Anderson at 488-4646. Thank you for your assistance.

EL:ep
Enclosures

cc: Lori Tinney
Senate Governmental Operations Committee

Lucy Bloom
House Science and Technology Committee

PLEASE RETURN BY NOVEMBER 21, 1988

The Florida Legislature
Joint Committee on Information
Technology Resources
805 First Florida Bank Building
Tallahassee, Florida 32301
(Inter-Agency Mail: c/o House of Representatives)
(904) 488-4646

Name: _____
Title: _____
Organization: _____

SURVEY OF COMPUTER MATCHING ACTIVITIES
IN STATE DEPARTMENTS

1. Has your department participated in computer matching activities[1] with another agency during the 1987-88 fiscal year?

Yes 11 No 16

If no, skip to Question #12.

If yes, how many matching programs has your department participated in during FY 1987-88?

6 1-5
2 6-10
1 11-15
____ more than 15

2. What method(s) is used to exchange records with another agency?

2 on-line
2 batch processing
18 exchange of computer tapes
1 exchange of hard copy
5 other (please specify)
1 each = manual operation; floppy disk; computer voice response over telephone; file transfer program; electronic transfer

3. What is the total estimated number of records matched in your department in FY 1987-88?

State total = 18,060,854

---

[1] Defined as the computerized comparison of two or more automated systems of records to identify individuals common to two or more of the record systems [illegible] to one of the record systems. This includes the participation by either a matching agency (the agency performing the match) or a source agency (the agency disclosing records to the matching agency for use in the match).

4. Are cost-benefit analyses performed prior to computer matching programs?

Always ____ Sometimes 2 Never 6

1 not applicable - source agency

a. Are cost-benefit analyses performed after each matching program?

Always ____ Sometimes 2 Never 6

1 not applicable - source agency

b. Approximately how many pre- and post-match cost-benefit analyses have been completed?

7 none
2 1-5
____ 6-10
____ more than 10

5. Do the individual subjects of the match provide written consent prior to a match?

Always 1 Sometimes 1 Never 7

If yes, please attach a copy of the form which is used to obtain consent.

6. Are any of your matching programs required or authorized by legislation?

Yes 4 No 4 1 no response

If yes, please list matches required or authorized and cite the statutory authorization for each type of match. (Please use separate sheet if necessary.)

Type of Match	Statutory Authorization
1. See attached sheet	
2.	
3.	

APPENDIX B-2

7. Have written procedures been developed to ensure that the files to be matched contain accurate information?

Yes 5 No 4

8. Do you have written procedures for the department to follow once a "match" has occurred?

Yes 4 No 5

a. Is there an appeals process within the department for an individual to respond to an administrative action resulting from a "match"?

Yes 6 No 2
1 N/A

b. Have there been terminations of benefits based on erroneous information?

Yes 1 No 6
2 N/A

c. Have there been any administrative hearings concerning an action resulting from a matching program held in FY 1987-88?

Yes 2 No 4
2 N/A
If yes, how many? 1 no response

HRS - 10 DOT - < 5

d. Have there ever been any court challenges to the matching programs?

Yes 0 No 7
1 N/A
If yes, how many? 1 no response

9. If available, please provide an estimate of the average cost of the matching programs your department conducted in FY 1987-88.

Not available - 5
not applicable - 1
No response - 2
$500 - 1

10. If available, please provide an estimate of the average amount of money recovered/saved in FY 1987-88 through the use of computer matches.

Not available - 5
Not applicable - 1
No response - 2
$500,000 - 1 ("if we have to code data by hand")

11. Does your department have:

a. procedures for retention or destruction of records created by matching programs?

Yes 7 No 2

b. procedures for notifying individuals that any information they provide may be subject to verification through matching programs? Yes 2 No 7

c. procedures for ensuring security of the records matched?

Yes 5 No 4

d. procedures governing the use of records provided by the source agency for use in a matching program, including the return of records to the source agency or destruction of these records? Yes 6 No 3

e. written guidelines or policy statements on the duplication or redisclosure of records provided by the source agency within or outside of the recipient agency?

Yes 4 No 4
1 no response

f. written criteria to be used by department officials for evaluating whether or not a proposed match should be conducted? Yes 1 No 7
1 no response

If yes, how often are these criteria used?

Always 1 Sometimes ____ Never ____

12. Has your department used computerized front-end verification[2] at any time as part of the application process for participation in department programs or benefits?

Yes 4 No 5

If no, do you have plans to use front-end verification?

Yes ____ No 5

---

[2]Defined as the certification of the accuracy and authenticity of information supplied by an applicant by checking against similar information from another agency or source.

13. Has your department conducted any cost-benefit studies of front-end verification?

Yes 0 No 9

Responses to Question 6

Type of Match	Statutory Authorization
HRS	
1. Client Information System	Fla. Statutes, Chap. 409
2. Food Stamp System	"
3. Assistance Payments System	"
4. Department of Lottery	"
5. Dept. of Highway Safety & Motor Vehicles	"
6. Department of Corrections	"
7. Division of Public Assistance Fraud (Auditor General)	"
8. Dept. of Labor & Employment Security	"
9. Federal Parent Locator	Title IV-D, Federal Social Security Act
10. Internal Revenue Service	"
11. Income Matching	IEVS - 7. CFR 272.8 and Deficit Reduction Act, Section 2651
12. Unemployment Compensation Benefit Information	Deficit Reduction Act, Section 2651
13. Social Security Information	"
14. Alien Number Information	Immigration Reform and Control Act, Section 121
FDLE	
1. Concealed weapon permit applicants/convicted felons	s. 790.06(6)(a), F.S.
2. Missing juveniles/birth records of missing children	s. 937.024, F.S.
3. Missing juveniles/DOE	s. 937.023, F.S.
4. Concealed weapon permit holders/FCIC	s. 790.06(7), F.S.

Type of Match	Statutory Authorization
5. RAIS council project	87-243, Laws of Florida
DOE	
1. IRS Tax Refund Offset	31 USC 3716, Pub. 297-457
2. Federal Wage Garnishment Programs	PL 99-498, PL 100-50, Section 430(A)(a)(b)(e)
3. Community College Graduate/ leaves to Employer	s. 240.355, F.S.
4. Communinty College Graduate/ leaves to University	s. 240.355, F.S.
5. Voc. Ed. Follow-up	s. 240.355, F.S.
6. Individual records by demographic variables (For RAISCC)	Ch. 87-243, Laws of Florida
7. Teaching Certificates	Ch. 231, F.S.
8. SUS - FSU Acct's. Receivables	s. 17.29, F.S. 3A-21.004(a), F.A.C.
DOT	
1. Accident Analysis	s. 334.063, F.S.

JOHN W. VOGT
President

JON MILLS
Speaker

THE FLORIDA LEGISLATURE

JOINT COMMITTEE ON INFORMATION TECHNOLOGY RESOURCES

Senator George Stuart, Jr., Chair
Representative Anne Mackenzie, Vice-Chair

EDWIN A. LEVINE, STAFF DIRECTOR
805, First Florida Bank Building
215 South Monroe Street
Tallahassee, Florida 32301
Telephone (904) 488-4643

September 9, 1988

Dear State Official:

Staff of Florida's Joint Committee on Information Technology Resources are in the process of developing fair information practices legislation, which will be introduced by our chairman during the 1989 session of the Florida Legislature. It will be helpful to us in developing draft legislation to examine the experiences of other states with their information practices law. We are also gathering information on state agency computer matching activities.

I would appreciate your assistance in completing the enclosed questionnaire and returning it to me by October 10, 1988. I will provide copies of the completed staff report and draft legislation to all respondents. Enclosed is a copy of our 1987 report on fair information practices. Should you have any questions or comments, please call me or Sharon Anderson at (904)488-4646. Thank you for your help.

Sincerely,

Edwin A. Levine
Staff Director

Enclosures

States Responded: California
Connecticut
Indiana
Minnesota
New York
Ohio
Utah

The Florida Legislature
Information Technology Resources Committee
805 First Florida Bank Building
215 S. Monroe Street
Tallahassee, Florida 32301
(904) 488-4646

Name: _____

Title: _____

Agency: _____

Address: _____

_____

_____

Please return by October 10

SURVEY OF FAIR INFORMATION PRACTICES LEGISLATION AND COMPUTERIZED MATCHING ACTIVITIES IN OTHER STATES

1. Have any changes been made in your state's fair information practices legislation since it was first enacted?

   Yes 7 No 0

   If yes, please briefly describe the changes, and send a copy of your state's fair information practices legislation.

   _____

   _____

   _____

2. What is the estimated total number of inquiries from individuals each year to see personal information on themselves? 4 unknowns

   1 each = 1,000's
   > 3,000
   > 5,000

3. What is the estimated total number of inquiries from individuals each year to change personal information on themselves? 5 unknowns

   1 each = < 100
   169

4. Are most disputes regarding fair information practices resolved between the agency and the individual, or are they appealed to an outside authority?

   6 Resolved between agency and individual
   _____ Appealed to outside authority

   1 unknown

5. What is the average number per year of informal disputes that are appealed to an outside authority, but resolved without a formal hearing?

1 none
3 1 - 25
____ 26 - 50
____ 51 - 75
____ 76 - 100
____ more than 100
2 unknown
1 See statistics in report

What type of dispute was most frequent?

2 Access to records
1 Request to change records
1 Other (Please specify) wrongful disclosures
2 unknown
1 See statistics in report

6. Please estimate the number of formal hearings that have been held to resolve fair information practices disputes since implementation of your state's legislation?

2 none
____ 1 - 5
2 6 - 10
____ 11 - 20
____ more than 20
2 unknown 1 See statistics in report

What type of dispute was most frequent?

1 Access to records
1 Request to change records
____ Other (Please specify _____

7. Please estimate the number of individuals who have gone to court over a dispute to date?

1 none
4 1 - 5
____ 6 - 10
____ 11 - 20
2 more than 20

How many damage awards have been made and what was the amount of each award?

		AMOUNT
4	none	
	1	$
	2	$
	3	$
	4	$
	5 or more	$
	3 unknown	

8. Please identify in rank order the three groups which generate the highest number of requests for information, or disputes (1 being the highest).

1	Public assistance recipients (e.g., food stamps, AFDC, medicaid, etc.)
1	Professional and occupational licensees
2	Current state personnel
2	Former state personnel
1	State employment applicants
	Motor vehicle registrants
	State hospital patients
3	Prisoners
	Students
5	Other (Please specify)

1 each = Taxpayers; General public; Local government personnel; child abuse; media

2 unknown

9. Are the records of professional and occupational licensees subject to the provisions of your state's fair information practices act?

7 Yes 0 No

If yes, what is the average total number of requests each year, at the agency level, from professional and occupational licensees regarding their personal information?

	none
	1 - 5
	6 - 10
	11 - 20
1	21 - 50
	more than 50
	6 unknown

How many requests were appealed to an outside authority each year?

1 none
1 1 - 5
____ 6 - 10
____ 11 - 20
1 more than 20
4 unknown

10. Are agencies required to publish reports on disclosures of personal information?

4 Yes 3 No

If yes, where are they published?

_____

What information is included in the reports?

_____

_____

_____

11. Is there a notification requirement for personal information requested of clients over the telephone?

1 Yes 6 No

If yes, how is this requirement met?

X Verbally over the telephone
X Written follow-up notice
X Other (please specify) Contained on data collection forms

_____

12. Have any funds to carry out the legislation ever been appropriated since its implementation?

Yes 2 No 4 1 no records available. Some agencies asked for budget augmentation in FY 78-79.

If yes, what amount has been appropriated specifically for the fair information practices legislation? $50,000 - $100,000 Annually - Privacy Division only
$25,000 - Start up appropriation

Have any employee positions ever been established to carry out the legislation since its implementation?

Yes 5 No 2

If yes, how many new positions were established?

5 1 - 5
____ 6 - 10
____ 11 - 20
____ more than 20

What are the estimated annual costs associated with your state's fair information practices legislation?

1 each = Varies by agency - "data incomplete & of doubtful accuracy"; blank; $500,000 - includes local government - most costs associated with personnel time; $1,000; approx. $20,000 (2 unable to calculate)

13. Do state agencies participate in any computer matching activities? (Defined as the computerized comparison of two or more systems of records to identify individuals common to two or more of the record systems or unique to one of the record systems.)

Yes 6 No ____ 1 unknown

If yes, what is the estimated number of matching programs conducted per year?

2 1 - 5
1 6 - 10
1 11 - 20
1 21 - 30
____ 31 - 50
____ more than 50
2 unknown

14. Listed below are the general categories of computer matching programs covered by the proposed federal Computer Matching and Privacy Protection Act of 1988. For your state, please indicate the estimated number of computer matching programs in each of these or any other categories. (Could choose more than one)

4 Establish or verify eligibility for a government benefit program
4 Recoup payments or delinquent debts under a government benefit program
____ Other (Please specify)

_____

_____

3 unknown

15. Are cost-benefit analyses of computer matching programs ever done either prior to or after the matching programs?

Yes 2 No 3

2 unknown

If yes, are the cost-benefit analyses legislatively required?

Yes _____ No 2

If available, please provide a copy of two recent cost-benefit analyses.

16. Have you passed legislation regulating computer matching in your state?

Yes 1 No 6

If yes, please send a copy of the legislation.

17. Are any state agencies and/or programs conducting computerized front-end verification for eligibility to a benefit program? (Defined as certification of the accuracy and authenticity of information given by an applicant by checking against similar information from another agency or source.)

Yes 4 No _____ 3 unknown

If yes, which agencies and/or programs?

1. Dept. of Social Services; Unemployment Ins.
2. Dept. Human Services; Dept. of Jobs & Training
3. Social Services; Tax, Labor, Health
4. Ohio Student Loan Commission

If available, please provide a copy of two recent agency reports on their use of front-end verification.

18. Are any computer matching or front end verification programs required or authorized by state or federal legislation?

Yes 3 No 4

If yes, please list the programs required or authorized and cite the statute for each type of match

1. Unemployment Insurance, Social Welfare - Federal Stat.
2. (Programs not listed)
3. Several - Many related to tax, public assistance, unemployment, medicaid, student loans, etc.

APPENDIX C

PUBLIC HEARINGS AGENDAS

BOB CRAWFORD
President

TOM GUSTAFSON
Speaker

THE FLORIDA LEGISLATURE

JOINT COMMITTEE ON INFORMATION TECHNOLOGY RESOURCES

Senator George Stuart, Jr., Chair
Representative Susan Guber, Vice-Chair

EDWIN A. LEVINE, STAFF DIRECTOR
805, First Florida Bank Building
215 South Monroe Street
Tallahassee, Florida 32301
Telephone (904) 488-4646

Public Hearing
"The States Information Policy: Responses to Changes in an Electronic Age"

Committee Room A, Senate Office Building
Tallahassee
January 9, 1989

10:00 a.m.
Opening Remarks — Senator George Stuart, Jr.

* Dorothy Joyce
Department of State

* Roy Saltman
National Institute of Standards and Technology

Dave Mann
Department of State

* Randy Esser
Department of Highway Safety & Motor Vehicles

* Robert MacNeel & Ray Seidel
Montgomery Co., PA

* Barratt Wilkins
Department of State

* Ed Johnson
Information & Records Engineering, Inc.

Open Testimony

* Steven Dopp
Interested citizen

12:00 noon
Adjournment

* Indicates written remarks or other written materials were provided to the Committee

BOB CRAWFORD
President

TOM GUSTAFSON
Speaker

THE FLORIDA LEGISLATURE

JOINT COMMITTEE ON INFORMATION TECHNOLOGY RESOURCES

Senator George Stuart, Jr., Chair
Representative Susan Guber, Vice-Chair

EDWIN A. LEVINE, STAFF DIRECTOR
805, First Florida Bank Building
215 South Monroe Street
Tallahassee, Florida 32301
Telephone (904) 488-4646

Public Hearing
"The State's Information Policy: Response to Change in an Electronic Age"

Broward County Commission Chambers
Ft. Lauderdale
January 18, 1989

9:00 a.m.
Opening Remarks — Senator George Stuart, Jr.

* Jane Carroll
Supervisor of Elections
Broward Co.

* Jacqueline Winchester
Supervisor of Elections,
Palm Beach County

* David Leahy
Supervisor of Elections,
Dade County

Robert Ginsberg
Metro-Dade County

* Alan Westin
Reference Point Foundation

Jerry Berman
American Civil Liberties Union

* Robert Ellis Smith
Privacy Journal

Thomas McGovern, Consultant
Clerk of the Courts, Dade County

12:00 noon - 1:00 p.m.
Lunch

1:00 p.m.

* Ken Wilkinson
Property Appraiser, Lee County

* Ron Plesser
Information Industry Association

Lawrence Culligan
West Publishing Company

* Gerald Yung
Mead Data Central

* Lee Holroyd
City of Fort Lauderdale

Open Testimony

P.J. Ponder
Information Resource Commission

Joanne Ennis
Broward County

3:00 p.m.
Adjournment

* Indicates written remarks or other written materials were provided to the Committee

BOB CRAWFORD
President

TOM GUSTAFSON
Speaker

THE FLORIDA LEGISLATURE

JOINT COMMITTEE ON INFORMATION TECHNOLOGY RESOURCES

Senator George Stuart, Jr., Chair
Representative Susan Guber, Vice-Chair

EDWIN A. LEVINE, STAFF DIRECTOR
805, First Florida Bank Building
215 South Monroe Street
Tallahassee, Florida 32301
Telephone (904) 488-4646

Public Hearing
"The State's Information Policy: Responses to Changes in an Electronic Age"

Orlando City Council Chambers
Orlando
January 19, 1989

10:00 a.m.
Opening Remarks — Senator George Stuart, Jr.

* James Nelson
  Kentucky Dept. for Libraries and Archives
* Robin Krivanek
  Supervisor of Elections, Hillsborough Co.
* Betty Carter
  Supervisor of Elections, Orange Co.
* Beatrice Polk
  Former candidate for Supervisor of Elections, Brevard Co.

12:00 noon - 1:00 p.m.
Lunch

1:00 p.m.

* Fred Wood
U.S. Congress, Office of
Technology Assessment

* Frank Perkins, Gary Knuckles,
and Dale Friedly
Manatee County Property
Appraiser's Office

Open Testimony

* Terrell Redden
St. Lucie County

John Mikos
Sarasota County Property
Appraiser

Alfred Leiser
Pinellas County

3:00 p.m.
Adjournment

* Indicates written remarks or other written materials were provided to the Committee

APPENDIX D

LAWS AND OPINIONS RELATED TO THE COPYRIGHT OF PUBLIC SOFTWARE

CHAPTER 119

PUBLIC RECORDS

119.01 General state policy on public records.
119.011 Definitions.
119.0115 Videotapes and video signals, exemption from chapter.
119.012 Records made public by public fund use.
119.02 Penalty.
119.021 Custodian designated.
119.031 Keeping records in safe places, copying or repairing certified copies.
119.041 Destruction of records regulated.
119.05 Disposition of records at end of official's term.
119.06 Demanding custody.
119.07 Inspection and examination of records, exemptions.
119.072 Criminal intelligence or investigative information obtained from out-of-state agencies.
119.08 Photographing public records.
119.085 Remote electronic access to public records.
119.09 Assistance of the Division of Library and Information Services, records and information management program, of the Department of State.
119.092 Registration by federal employer's registration number.
119.10 Violation of chapter; penalties.
119.11 Accelerated hearing; immediate compliance.
119.12 Attorney's fees.
119.14 Periodic legislative review of exemptions from public meeting and public record requirements.

119.01 General state policy on public records.—

(1) It is the policy of this state that all state, county, and municipal records shall at all times be open for a personal inspection by any person.

(2) All agencies shall establish a program for the disposal of records that do not have sufficient legal, fiscal, administrative, or archival value in accordance with retention schedules established by the records and information management program of the Division of Library and Information Services of the Department of State.

History.—s. 1, ch. 5942, 1909; RGS 424; CGL 490; s. 1, ch. 73-98; s. 2, ch. 75-225; s. 2, ch. 83-286; s. 4, ch. 86-163.

cf.—s. 119.14 Periodic legislative review of exemptions from public meeting and record requirements.
s. 400.321 Confidentiality.

119.011 Definitions.—For the purpose of this chapter:

(1) "Public records" means all documents, papers, letters, maps, books, tapes, photographs, films, sound recordings or other material, regardless of physical form or characteristics, made or received pursuant to law or ordinance or in connection with the transaction of official business by any agency.

(2) "Agency" means any state, county, district, authority, or municipal officer, department, division, board, bureau, commission, or other separate unit of government created or established by law and any other public or private agency, person, partnership, corporation, or business entity acting on behalf of any public agency.

(3)(a) "Criminal intelligence information" means information with respect to an identifiable person or group of persons collected by a criminal justice agency in an effort to anticipate, prevent, or monitor possible criminal activity.

(b) "Criminal investigative information" means information with respect to an identifiable person or group of persons compiled by a criminal justice agency in the course of conducting a criminal investigation of a specific act or omission, including, but not limited to, information derived from laboratory tests, reports of investigators or informants, or any type of surveillance.

(c) "Criminal intelligence information" and "criminal investigative information" shall not include:

1. The time, date, location, and nature of a reported crime.

2. The name, sex, age, and address of a person arrested or of the victim of a crime except as provided in s. 119.07(3)(h).

3. The time, date, and location of the incident and of the arrest.

4. The crime charged.

5. Documents given or required by law or agency rule to be given to the person arrested, except as provided in s. 119.07(3)(h), and

6. Informations and indictments except as provided in s. 905.26.

(d) The word "active" shall have the following meaning:

1. Criminal intelligence information shall be considered "active" as long as it is related to intelligence gathering conducted with a reasonable, good faith belief that it will lead to detection of ongoing or reasonably anticipated criminal activities.

2. Criminal investigative information shall be considered "active" as long as it is related to an ongoing investigation which is continuing with a reasonable, good faith anticipation of securing an arrest or prosecution in the foreseeable future.

In addition, criminal intelligence and criminal investigative information shall be considered "active" while such information is directly related to pending prosecutions or appeals. The word "active" shall not apply to information in cases which are barred from prosecution under the provisions of s. 775.15 or other statute of limitation.

(4) "Criminal justice agency" means any law enforcement agency, court, or prosecutor. The term also includes any other agency charged by law with criminal law enforcement duties, or any agency having custody of criminal intelligence information or criminal investigative information for the purpose of assisting such law enforcement agencies in the conduct of active criminal investigation or prosecution or for the purpose of litigating civil actions under the Racketeer Influenced and Corrupt Organization Act, during the time that such agencies are in possession of criminal intelligence information or crim-

inal investigative information pursuant to their criminal law enforcement duties.

History.—s. 1, ch. 67-125; s. 2, ch. 73-98; s. 3, ch. 75-225; ss. 1, 2, ch. 79-187; s. 8, ch. 85-53.

[illegible]—ss. 895.01-895.06, Florida RICO (Racketeer Influenced and Corrupt Organization) Act.

119.0115 Videotapes and video signals; exemption from chapter.—Any videotape or video signal which, under an agreement with an agency, is produced, made, or received by, or is in the custody of, a federally licensed radio or television station or its agent is exempt from this chapter.

History.—s. 1, ch. 80-1.

119.012 Records made public by public fund use.—If public funds are expended by an agency defined in s. 119.011(2) in payment of dues or membership contributions to any person, corporation, foundation, trust, association, group, or other organization, then all the financial, business and membership records pertaining to the public agency from which or on whose behalf the payments are made, of the person, corporation, foundation, trust, association, group, or organization to whom such payments are made shall be public records and subject to the provisions of s. 119.07.

History.—s. 3, ch. 75-225.

[illegible]—s. 960.28, Payment for victims' initial examinations.

119.02 Penalty.—A public officer who knowingly violates the provisions of s. 119.07(1) is subject to suspension and removal or impeachment and, in addition, is guilty of a misdemeanor of the first degree, punishable as provided in s. 775.082 or s. 775.083.

History.—s. 2, ch. 5942, 1909; RGS 425; CGL 491; s. 1, ch. 17173, 1935; CGL 1936 Supp. 7520(6); s. 73, ch. 71-136; s. 6, ch. 75-225; s. 4, ch. 84-298.

119.021 Custodian designated.—The elected or appointed state, county, or municipal officer charged with the responsibility of maintaining the office having public records, or his designee, shall be the custodian thereof.

History.—s. 2, ch. 67-125; s. 3, ch. 83-286.

119.031 Keeping records in safe places; copying or repairing certified copies.—Insofar as practicable, custodians of vital, permanent, or archival records shall keep them in fireproof and waterproof safes, vaults, or rooms fitted with noncombustible materials and in such arrangement as to be easily accessible for convenient use. All public records should be kept in the buildings in which they are ordinarily used. Record books should be copied or repaired, renovated, or rebound if worn, mutilated, damaged, or difficult to read. Whenever any state, county, or municipal records are in need of repair, restoration, or rebinding, the head of such state agency, department, board, or commission, the board of county commissioners of such county, or the governing body of such municipality may authorize that such records be removed from the building or office in which such records are ordinarily kept for the length of time required to repair, restore, or rebind them. Any public official who causes a record book to be copied shall attest it and certify on oath that it is an accurate copy of the original book. The copy shall then have the force and effect of the original.

History.—s. 3, ch. 67-125; s. 4, ch. 83-286.

119.041 Destruction of records regulated.—Every public official shall systematically dispose of records no longer needed subject to the consent of the records and information management program of the Division of Library and Information Services of the Department of State in accordance with s. 257.36.

History.—s. 4, ch. 67-125; ss. 10, 35, ch. 69-106; s. 5, ch. 83-286; s. 5, ch. 86-163.

119.05 Disposition of records at end of official's term.—Whoever has the custody of any public records shall, at the expiration of his term of office, deliver to his successor or, if there be none, to the records and information management program of the Division of Library and Information Services of the Department of State all records, books, writings, letters, and documents kept or received by him in the transaction of his official business.

History.—s. 5, ch. 67-125; ss. 10, 35, ch. 69-106; s. 6, ch. 86-163.

119.06 Demanding custody.—Whoever is entitled to the custody of public records shall demand them from any person having illegal possession of them, who shall forthwith deliver the same to him. Any person unlawfully possessing public records shall upon demand of any person and within 10 days deliver such records to their lawful custodian unless just cause exists for failing to deliver such records.

History.—s. 6, ch. 67-125.

119.07 Inspection and examination of records; exemptions.—

(1)(a) Every person who has custody of a public record shall permit the record to be inspected and examined by any person desiring to do so, at any reasonable time, under reasonable conditions, and under supervision by the custodian of the public record or his designee. The custodian shall furnish a copy or a certified copy of the record upon payment of the fee prescribed by law or, if a fee is not prescribed by law, upon payment of the actual cost of duplication of the record. The phrase "actual cost of duplication" means the cost of the material and supplies used to duplicate the record, but it does not include the labor cost or overhead cost associated with such duplication. However, the charge for copies of county maps or aerial photographs supplied by county constitutional officers may also include a reasonable charge for the labor and overhead associated with its duplication. Unless otherwise provided by law, the fees to be charged for duplication of public records shall be collected, deposited, and accounted for in the manner prescribed for other operating funds of the agency.

(b) If the nature or volume of public records requested to be inspected, examined, or copied pursuant to this subsection is such as to require extensive use of information technology resources or extensive clerical or supervisory assistance by personnel of the agency involved, or both, the agency may charge, in addition to the actual cost of duplication, a special service charge, which shall be reasonable and shall be based on the cost incurred for such extensive use of information technology resources or the labor cost of the personnel providing the service that is actually incurred by the agency

or attributable to the agency for the clerical and supervisory assistance required, or both. "Information technology resources" shall have the same meaning as in s. 282.303(10).

(c) When ballots are produced under this section for inspection or examination, no persons other than the supervisor of elections or his employees shall touch the ballots. The supervisor of elections shall make a reasonable effort to notify all candidates by telephone or otherwise of the time and place of the inspection or examination. All such candidates, or their representatives, shall be allowed to be present during the inspection or examination.

(2)(a) A person who has custody of a public record and who asserts that an exemption provided in subsection (3) or in a general or special law applies to a particular public record or part of such record shall delete or excise from the record only that portion of the record with respect to which an exemption has been asserted and validly applies, and such person shall produce the remainder of such record for inspection and examination. If the person who has custody of a public record contends that the record or part of it is exempt from inspection and examination, he shall state the basis of the exemption which he contends is applicable to the record, including the statutory citation to an exemption created or afforded by statute, and, if requested by the person seeking the right under this subsection to inspect, examine, or copy the record, he shall state in writing and with particularity the reasons for his conclusion that the record is exempt.

(b) In any civil action in which an exemption to subsection (1) is asserted, if the exemption is alleged to exist under or by virtue of paragraph (e), paragraph (f), paragraph (g), paragraph (m), paragraph (o), or paragraph (r) of subsection (3), the public record or part thereof in question shall be submitted to the court for an inspection in camera. If an exemption is alleged to exist under or by virtue of paragraph (d) of subsection (3), an inspection in camera will be discretionary with the court. If the court finds that the asserted exemption is not applicable, it shall order the public record or part thereof in question to be immediately produced for inspection, examination, or copying as requested by the person seeking such access.

(c) Even if an assertion is made by the custodian of a public record that a requested record is not a public record subject to public inspection and examination under subsection (1), the requested record shall, nevertheless, not be disposed of for a period of 30 days after the date on which a written request requesting the right to inspect, examine, or copy the record was served on or otherwise made to the custodian of the record by the person seeking access to the record. If a civil action is instituted within the 30-day period to enforce the provisions of this section with respect to the requested record, the custodian shall not dispose of the record except by order of a court of competent jurisdiction after notice to all affected parties.

(d) The absence of a civil action instituted for the purpose stated in paragraph (c) will not relieve the custodian of his duty to maintain the record as a public record if the record is in fact a public record subject to public inspection and examination under subsection (1) and will not otherwise excuse or exonerate the custodian from any unauthorized or unlawful disposition of such record.

(3)(a) All public records which are presently provided by law to be confidential or which are prohibited from being inspected by the public, whether by general or special law, are exempt from the provisions of subsection (1).

(b) All public records referred to in ss. 199.222, 228.093, 257.261, 288.075, 624.319(3) and (4), and 655.057(1)(b), (3), and (4) are exempt from the provisions of subsection (1).

(c) Examination questions and answer sheets of examinations administered by a governmental agency for the purpose of licensure, certification, or employment are exempt from the provisions of subsection (1). A person who has taken such an examination shall have the right to review his own completed examination.

(d) Active criminal intelligence information and active criminal investigative information are exempt from the provisions of subsection (1).

(e) Any information revealing the identity of a confidential informant or a confidential source is exempt from the provisions of subsection (1).

(f) Any information revealing surveillance techniques or procedures or personnel is exempt from the provisions of subsection (1). Notwithstanding s. 119.14, any comprehensive inventory of state and local law enforcement resources compiled pursuant to part I, chapter 23, and any comprehensive policies or plans compiled by a criminal justice agency pertaining to the mobilization, deployment, or tactical operations involved in responding to emergencies, as defined in s. 252.34(2), are exempt from the provisions of subsection (1) and unavailable for inspection, except by personnel authorized by a state or local law enforcement agency, the office of the Governor, the Department of Legal Affairs, the Department of Law Enforcement, or the Department of Community Affairs as having an official need for access to the inventory or comprehensive policies or plans. This exemption is subject to the Open Government Sunset Review Act in accordance with s. 119.14.

(g) Any information revealing undercover personnel of any criminal justice agency is exempt from the provisions of subsection (1).

(h) Any criminal intelligence information or criminal investigative information including the photograph, name, address, or other fact or information which reveals the identity of the victim of the crime of sexual battery as defined in chapter 794; the identity of the victim of the crime of lewd, lascivious, or indecent assault upon or in the presence of a child, as defined in chapter 800; or the identity of the victim of the crime of child abuse as defined by chapter 827 and any criminal intelligence information or criminal investigative information or other criminal record, including those portions of court records, which may reveal the identity of a person under the age of 18 who is a victim of any sexual offense, including a sexual offense proscribed in chapter 794, chapter 800, or chapter 827, is exempt from the provisions of subsection (1)

(i) Any criminal intelligence information or criminal investigative information which reveals the personal assets of the victim of a crime, other than property stolen or destroyed during the commission of the crime, is exempt from the provisions of subsection (1).

(j) All criminal intelligence and criminal investigative information received by a criminal justice agency prior to January 25, 1979, is exempt from the provisions of subsection (1).

(k) The home addresses, telephone numbers, and photographs of active or former law enforcement personnel; the home addresses, telephone numbers, photographs, and places of employment of the spouses and children of active or former law enforcement personnel; and the names and locations of schools attended by the children of active or former law enforcement personnel are exempt from the provisions of subsection (1).

(l) Any information provided to an agency of state government or to an agency of a political subdivision of the state for the purpose of forming ridesharing arrangements, which information reveals the identity of an individual who has provided his name for ridesharing arrangements as defined in s. 341.031(6), is exempt from the provisions of subsection (1).

(m) Any information revealing the substance of a confession of a person arrested is exempt from the provisions of subsection (1), until such time as the criminal case is finally determined by adjudication, dismissal, or other final disposition.

(n) A patient record obtained by the Hospital Cost Containment Board established under s. 395.503, which record contains the name, residence or business address, telephone number, social security or other identifying number, or photograph of any person or the spouse, relative, or guardian of such person or which record is patient-specific or otherwise identifies the patient, either directly or indirectly, is exempt from the provisions of paragraph (1)(a).

(o) A public record which was prepared by an agency attorney (including an attorney employed or retained by the agency or employed or retained by another public officer or agency to protect or represent the interests of the agency having custody of the record) or prepared at the attorney's express direction, which reflects a mental impression, conclusion, litigation strategy, or legal theory of the attorney or the agency, and which was prepared exclusively for civil or criminal litigation or for adversarial administrative proceedings, or which was prepared in anticipation of imminent civil or criminal litigation or imminent adversarial administrative proceedings, is exempt from the provisions of subsection (1) until the conclusion of the litigation or adversarial administrative proceedings. When asserting the right to withhold a public record pursuant to this paragraph, the agency shall identify the potential parties to any such criminal or civil litigation or adversarial administrative proceedings. If a court finds that the document or other record has been improperly withheld under this paragraph, the party seeking access to such document or record shall be awarded reasonable attorney's fees and costs in addition to any other remedy ordered by the court.

(p) Sealed bids or proposals received by an agency pursuant to invitations to bid or requests for proposals are exempt from the provisions of subsection (1) until such time as the bids or proposals are opened.

(q) In any case in which an agency of the executive branch of state government seeks to acquire real property by purchase or through the exercise of the power of eminent domain all appraisals, other reports relating to value, offers, and counteroffers must be in writing and are exempt from the provisions of s. 119.01 and subsection (1) until execution of a valid option contract or a written offer to sell which has been conditionally accepted by the agency, at which time the exemption shall expire. The agency shall not finally accept the offer for a period of 30 days in order to allow public review of the transaction. The agency may give conditional acceptance to any option or offer subject only to final acceptance by the agency after the 30-day review period. If a valid option contract is not executed, or if a written offer to sell is not conditionally accepted by the agency, then the exemption from the provisions of this chapter shall expire at the conclusion of the condemnation litigation of the subject property. Nothing in this section shall be construed to provide an exemption from or exception to s. 286.011. For the purpose of this paragraph "option contract" means an agreement of an agency of the executive branch of state government to purchase real property subject to final agency approval. This paragraph shall have no application to other exemptions from the requirements of s. 119.01 or subsection (1) which are contained in other provisions of law and shall not be construed to be an express or implied repeal thereof.

(r) Data processing software obtained by an agency under a licensing agreement which prohibits its disclosure and which software is a trade secret, as defined in s. 812.081, and agency-produced data processing software which is sensitive are exempt from the provisions of subsection (1). The designation of agency-produced software as sensitive shall not prohibit an agency head from sharing or exchanging such software with another public agency. As used in this paragraph:

1. "Data processing software" has the same meaning as in s. 282.303(6).

2. "Sensitive" means only those portions of data processing software, including the specifications and documentation, used to:

a. Collect, process, store, and retrieve information which is exempt from the provisions of subsection (1);

b. Collect, process, store, and retrieve financial management information of the agency, such as payroll and accounting records; or

c. Control and direct access authorizations and security measures for automated systems.

(s) The names, addresses, and amounts contributed by donors to the state Fine Arts Endowment Program or to a local organization's fine arts endowment program fund created pursuant to s. 265.606 shall, at the request of the donor, be exempt from the provisions of subsection (1).

(t) A patient record obtained by the Department of Health and Rehabilitative Services pursuant to s. 641.27 from a health maintenance organization or from a provider of a health maintenance organization as to subscrib-

ers treated by the provider pursuant to a provider contract with a health maintenance organization, which record contains the name, the residential or business address, the telephone, social security, or other identifying number, or a photograph of any subscriber or of the spouse, relative, or guardian of the subscriber, or which record is patient-specific or otherwise identifies the patient, either directly or indirectly, is exempt from the provisions of subsection (1).

(u) A report obtained by the Department of Insurance from a health maintenance organization pursuant to s. 641.311, to the extent that such report contains the name, the residential or business address, the telephone, social security, or other identifying number, or a photograph of any subscriber or of the spouse, relative, or guardian of the subscriber, or other subscriber-identifying information, is exempt from the provisions of subsection (1).

(v) All complaints and other records in the custody of any unit of local government which relate to a complaint of discrimination relating to race, color, religion, sex, national origin, age, handicap, marital status, sale or rental of housing, the provision of brokerage services, or the financing of housing shall be exempt from the provisions of subsection (1) until a finding is made relating to probable cause, the investigation of the complaint becomes inactive, or the complaint or other record is made part of the official record of any hearing or court proceeding. This provision shall not affect any function or activity of the Florida Commission on Human Relations. Any state or federal agency which is authorized to have access to such complaints or records by any provision of law shall be granted such access in the furtherance of such agency's statutory duties, notwithstanding the provisions of this section. This paragraph shall not be construed to modify or repeal any special or local act. This exemption is subject to the Open Government Sunset Review Act in accordance with s. 119.14.

(w) All complaints and other records in the custody of any agency in the executive branch of state government which relate to a complaint of discrimination relating to race, color, religion, sex, national origin, age, handicap, or marital status in connection with hiring practices, position classifications, salary, benefits, discipline, discharge, employee performance, evaluation, or other related activities shall be exempt from the provisions of subsection (1) until a finding is made relating to probable cause, the investigation of the complaint becomes inactive, or the complaint or other record is made part of the official record of any hearing or court proceeding. This provision shall not affect any function or activity of the Florida Commission on Human Relations. Any state or federal agency which is authorized to have access to such complaints or records by any provision of law shall be granted such access in the furtherance of such agency's statutory duties, notwithstanding the provisions of this section. This exemption is subject to the Open Government Sunset Review Act in accordance with s. 119.14.

(x) A patient record obtained from a hospital by the Department of Health and Rehabilitative Services or its agent pursuant to s. 395.031, which record contains the name, residence or business address, telephone number, social security or other identifying number, or photograph of any person or the spouse, relative, or guardian of such person or which record is patient-specific or otherwise identifies the patient, either directly or indirectly is exempt from the provisions of subsection (1).

(4) Nothing in this section shall be construed to exempt from subsection (1) a public record which was made a part of a court file and which is not specifically closed by order of court, except as provided in paragraphs (e), (f), (g), (m), (o), and (r) of subsection (3) and except information or records which may reveal the identity of a person under the age of 18 who is a victim of a sexual offense as provided in paragraph (h) of subsection (3).

(5) Nothing in subsection (3) shall be interpreted as providing an exemption from or exception to s. 286.011.

(6) The provisions of this section are not intended to expand or limit the provisions of Rule 3.220, Florida Rules of Criminal Procedure, regarding the right and extent of discovery by the state or by a defendant in a criminal prosecution.

History.—s. 7, ch. 67-125; s. 4, ch. 75-225; s. 2, ch. 77-60; s. 2, ch. 77-75; s. 2, ch. 77-94; s. 2, ch. 77-156; s. 2, ch. 78-81; ss. 2, 4, 6, ch. 79-187; s. 2, ch. 80-2; s. 1, ch. 81-245; s. 1, ch. 82-95; s. 36, ch. 82-243; s. 6, ch. 83-215; s. 2, ch. 83-258; s. 1, ch. 83-286; s. 5, ch. 84-298; s. 1, ch. 85-18; s. 1, ch. 85-45; s. 1, ch. 85-73; s. 1, ch. 85-86; s. 7, ch. 85-152; s. 1, ch. 85-177; s. 4, ch. 85-301; s. 2, ch. 86-1; s. 1, ch. 86-21; s. 1, ch. 86-109.

[1]Note.—The reference to "s. 282.303(10)" was substituted by the editors for a reference to "s. 282.303(8)" to conform to the renumbering by s. 17, ch. 87-137.

[2]Note.—The word "or" was substituted by the editors for the word "and."

[3]Note.—The reference to "s. 282.303(6)" was substituted by the editors for a reference to "s. 282.303(5)" to conform to the renumbering by s. 17, ch. 87-137.

Note.—Additional exemptions from the application of this section are indexed in Volume 4 of this edition in the General Index under the heading "Public Records."

119.072 Criminal intelligence or investigative information obtained from out-of-state agencies.—Whenever criminal intelligence information or criminal investigative information held by a non-Florida criminal justice agency is available to a Florida criminal justice agency, only on a confidential or similarly restricted basis, the Florida criminal justice agency may obtain and use such information in accordance with the conditions imposed by the providing agency.

History.—s. 3, ch. 79-187.

119.08 Photographing public records.—

(1) In all cases where the public or any person interested has a right to inspect or take extracts or make copies from any public record, instruments or documents, any person shall hereafter have the right of access to said records, documents or instruments for the purpose of making photographs of the same while in the possession, custody and control of the lawful custodian thereof, or his authorized deputy.

(2) Such work shall be done under the supervision of the lawful custodian of the said records, who shall have the right to adopt and enforce reasonable rules governing the said work. Said work shall, where possible, be done in the room where the said records, documents or instruments are by law kept, but if the same in the judgment of the lawful custodian of the said records, documents or instruments be impossible or impracticable, then the said work shall be done in such other room or place as nearly adjacent to the room where the said records, documents and instruments are kept as determined by the lawful custodian thereof

APPENDIX D-1

251

(3) Where the providing of another room or place is necessary, the expense of providing the same shall be paid by the person desiring to photograph the said records, instruments or documents. While the said work hereinbefore mentioned is in progress, the lawful custodian of said records may charge the person desiring to make the said photographs for the services of a deputy of the lawful custodian of said records, documents or instruments to supervise the same, or for the services of the said lawful custodian of the same in so doing at a rate of compensation to be agreed upon by the person desiring to make the said photographs and the custodian of the said records, documents or instruments, or in case the same fail to agree as to the said charge, then by the lawful custodian thereof.

History.—s. 8, ch. 67-125.

119.085 Remote electronic access to public records.—

(1) As an additional means of inspecting, examining, and copying public records of the executive branch, judicial branch, or any political subdivision of the state, public records custodians may provide access to the records by remote electronic means. The custodian shall charge a fee for remote electronic access, granted under a contractual arrangement with a user, which fee shall include the direct and indirect costs of providing such access. Fees for remote electronic access provided to the general public shall be in accordance with the provisions of s. 119.07(1). The custodian shall provide safeguards to protect the contents of public records from unauthorized remote electronic access or alteration and to prevent the disclosure or modification of those portions of public records which by general or special law are exempt from s. 119.07(1).

(2) This section is repealed on October 1, 1990, and shall be reviewed by the Legislature in advance of said date. In determining whether to reenact this section, the Legislature shall consider for the time period from July 1, 1985 through July 1, 1989:

(a) The number of the remote electronic access contracts which have been entered into by records custodians.

(b) Whether the fees charged have closely approximated the costs incurred in providing remote electronic access.

(c) Whether the security of the electronic records maintained by records custodians has been breached as a result of such access.

(d) Whether the provision of such access impaired the ability of records custodians to meet other public record requests.

History.—s. 2, ch. 85-86.

119.09 Assistance of the Division of Library and Information Services, records and information management program, of the Department of State.—The Division of Library and Information Services, records and information management program, of the Department of State shall have the right to examine into the condition of public records and shall give advice and assistance to public officials in the solution of their problems of preserving, creating, filing, and making available the public records in their custody. Public officials shall assist the division by preparing an inclusive inventory of categories of public records in their custody. The division shall establish a time period for the retention or disposal of each series of records. Upon the completion of the inventory and schedule, the division shall (subject to the availability of necessary space, staff, and other facilities for such purposes) make space available in its records center for the filing of semicurrent records so scheduled and in its archives for noncurrent records of permanent value and shall render such other assistance as needed, including the microfilming of records so scheduled.

History.—s. 9, ch. 67-125; ss. 10, 35, ch. 69-106; s. 6, ch. 83-286; s. 7, ch. 85-161.

119.092 Registration by federal employer's registration number.—Each state agency which registers or licenses corporations, partnerships, or other business entities shall include, by July 1, 1978, within its numbering system, the federal employer's identification number of each corporation, partnership, or other business entity registered or licensed by it. Any state agency may maintain a dual numbering system in which the federal employer's identification number or the state agency's own number is the primary identification number; however, the records of such state agency shall be designed in such a way that the record of any business entity is subject to direct location by the federal employer's identification number. The Department of State shall keep a registry of federal employer's identification numbers of all business entities, registered with the Division of Corporations, which registry of numbers may be used by all state agencies.

History.—s. 1, ch. 77-148.

119.10 Violation of chapter; penalties.—

(1) Any public officer who violates any provision of this chapter is guilty of a noncriminal infraction, punishable by fine not exceeding $500.

(2) Any person willfully and knowingly violating any of the provisions of this chapter is guilty of a misdemeanor of the first degree, punishable as provided in s. 775.082 or s. 775.083.

History.—s. 10, ch. 67-125; s. 74, ch. 71-136; s. 5, ch. 85-301.

119.11 Accelerated hearing; immediate compliance.—

(1) Whenever an action is filed to enforce the provisions of this chapter, the court shall set an immediate hearing, giving the case priority over other pending cases.

(2) Whenever a court orders an agency to open its records for inspection in accordance with this chapter, the agency shall comply with such order within 48 hours, unless otherwise provided by the court issuing such order, or unless the appellate court issues a stay order within such 48-hour period.

(3) A stay order shall not be issued unless the court determines that there is a substantial probability that opening the records for inspection will result in significant damage.

(4) Upon service of a complaint, counterclaim, or cross-claim in a civil action brought to enforce the provisions of this chapter, the custodian of the public record that is the subject matter of such civil action shall not

transfer custody, alter, destroy, or otherwise dispose of the public record sought to be inspected and examined, notwithstanding the applicability of an exemption or the assertion that the requested record is not a public record subject to inspection and examination under s. 119.07(1), until the court directs otherwise. The person who has custody of such public record may, however, at any time permit inspection of the requested record as provided in s. 119.07(1) and other provisions of law.
History.—s. 5, ch. 75-225, s. 2, ch. 83-214, s. 6, ch. 84-298

119.12 Attorney's fees.—

(1) If a civil action is filed against an agency to enforce the provisions of this chapter and if the court determines that such agency unlawfully refused to permit a public record to be inspected, examined, or copied, the court shall assess and award, against the agency responsible, the reasonable costs of enforcement including reasonable attorneys' fees.

(2) Whenever an agency appeals a court order requiring it to permit inspection of records pursuant to this chapter and such order is affirmed, the court shall assess a reasonable attorney's fee for the appeal against such agency.
History.—s. 5, ch. 75-225, s. 7, ch. 84-298

119.14 Periodic legislative review of exemptions from public meeting and public record requirements.—

(1) This section may be cited as the "Open Government Sunset Review Act."

(2) This act provides for the periodic automatic application of the policy of open government as provided in ss. 119.01 and 286.011 to certain exemptions from s. 286.011 and chapter 119. It is the intent of the Legislature that exemptions to s. 286.011 and chapter 119 shall be maintained only if:

(a) The exempted record or meeting is of a sensitive, personal nature concerning individuals;

(b) The exemption is necessary for the effective and efficient administration of a governmental program; or

(c) The exemption affects confidential information concerning an entity.

Thus, the maintenance or creation of an exemption must be compelled as measured by these criteria. Further, the Legislature finds that the public has a right to have access to executive branch governmental meetings and records unless the criteria in this act for restricting such access to a public meeting or public record are met and the criteria are considered during legislative review in connection with the particular exemption to be significant enough to override the strong public policy of open government. To strengthen the policy of open government, the Legislature shall consider the criteria in this act before enacting future exemptions.

(3)(a) On the dates specified in this subsection with respect to the chapters of law included in the titles of the Florida Statutes specified in this subsection, the provisions of ss. 119.01, 119.07(1), and 286.011 shall fully apply, notwithstanding any provisions in such chapters of law included in the titles of the Florida Statutes to the contrary, unless the application of this subsection to such chapters of law has been modified by subsequent law passed by the Legislature. The repeal dates and t tles of the Florida Statutes are as follows:

1. October 1, 1986, and at the end of each 10-yea period thereafter, with respect to chapters of law includ ed in titles I through V.

2. October 1, 1987, and at the end of each 10-yea period thereafter, with respect to chapters of law includ ed in titles VI through XI, except chapter 119 and ss 106.24, 106.25, 106.26, 106.27, 112.320, 112.321 112.322, and 112.324.

3. October 1, 1988, and at the end of each 10-yea period thereafter, with respect to chapters of law includ ed in titles XII through XVI.

4. October 1, 1989, and at the end of each 10-yea period thereafter, with respect to chapters of law includ ed in titles XVII through XXVIII.

5. October 1, 1990, and at the end of each 10-yea period thereafter, with respect to chapters of law includ ed in title XXIX.

6. October 1, 1991, and at the end of each 10-yea period thereafter, with respect to chapters of law includ ed in titles XXX through XXXII.

7. October 1, 1992, and at the end of each 10-yea period thereafter, with respect to chapters of law includ ed in titles XXXIII through XXXVI and title XXXVIII.

8. October 1, 1993, and at the end of each 10-yea period thereafter, with respect to chapters of law includ ed in title XXXVII.

9. October 1, 1994, and at the end of each 10-yea period thereafter, with respect to chapters of law includ ed in titles XXXIX through XLVII.

10. October 1, 1995, and at the end of each 10-yea period thereafter, with respect to:

a. Each exemption in chapter 119 which has not been reviewed in prior years because such exemption was not contained in those titles or because the exemption is generic in character and language and consequently applies to records created, maintained, or stored, by substantive language in two or more such t tles; and

b. Each exemption which is identified as being in two or more titles of the Florida Statutes by the Division of Statutory Revision.

(b) In the year prior to the repeal of an exemption pursuant to this section, the Division of Statutory Revision of the Joint Legislative Management Committee shall certify to the President of the Senate and the Speaker of the House of Representatives, by December 1, 1985, and by August 1 of each subsequent year, the language and statutory citation of each exemption scheduled for repeal the following year which meets the criteria of an exemption as defined in this act. Any exemption which is not identified and certified to the President of the Senate and the Speaker of the House of Representatives shall not be subject to legislative review and repeal under this act. If the division fails to certify an exemption which it subsequently determines should have been certified, it shall include such exemption in the following year's certification after such determination.

(c) An "exemption" is defined as a provision of the Florida Statutes which creates an exception to s. 119.01, s. 119.07(1), or s. 286.011 and which applies to the exec

utive branch of state government or to local government, but shall not include any provision of a special or local law.

(d) No exemption which is required by federal law shall be subject to repeal.

(4)(a) The Legislature shall conduct a review of the exemption prior to its scheduled repeal and shall consider as part of the review process the following:

1. What specific records or meetings are affected by the exemption?

2. Whom does the exemption uniquely affect, as opposed to the general public?

3. What is the identifiable public purpose or goal of the exemption?

4. Can the information contained in the records or discussed in the meeting be readily obtained by alternative means? If so, how?

(b) An exemption shall be maintained only if it serves an identifiable public purpose. An identifiable public purpose is served when the exemption meets one of the following purposes and such purpose is considered during legislative review in connection with the particular exemption being considered to be significant enough to override the strong public policy of open government:

1. Allows the state or its political subdivisions to effectively and efficiently administer a governmental program, which administration would be significantly impaired without the exemption;

2. Protects information of a sensitive personal nature concerning individuals, the release of which information would be defamatory to such individuals or cause unwarranted damage to the good name or reputation of such individuals or would jeopardize the safety of such individuals; or

3. Protects information of a confidential nature concerning entities, including, but not limited to, a formula, pattern, device, combination of devices, or compilation of information which is used to protect or further a business advantage over those who do not know or use it, the disclosure of which information would injure the affected entity in the marketplace.

(c) No records made prior to the date of a repeal of an exemption under this act shall be made public unless otherwise provided by law. In deciding whether such records shall be made public the Legislature shall consider whether the damage or loss to persons or entities uniquely affected by the exemption of the type specified in subparagraph (b)2. or subparagraph (b)3. would occur if the records were made public.

(d) Legislation which creates an exemption which is scheduled for repeal in the year it is enacted or the year following enactment shall not be subject to this act until the next review cycle for that title.

(e) An exemption that is created or revived and reenacted shall contain uniform language which clearly states the section in the Florida Statutes from which it is exempt, chapter 119 or s. 286.011. The uniform language shall also provide for the maximum public access to the meetings and records as is consistent with the purpose of the exemption. Each exemption shall also contain the statement: "This exemption is subject to the 'Open Government Sunset Review Act' in accordance with s. 119.14."

(f) In the year prior to the 1995 regular session, the Legislature shall consider the necessity of conducting further reviews of exemptions.

(g) Notwithstanding the provision of s. 768.28 or any other law, neither the state or its political subdivisions nor any other public body shall be made party to any suit in any court or incur any liability for the repeal or revival and reenactment of any exemption pursuant to this act. The failure of the Legislature to comply strictly with this section shall not invalidate an otherwise valid reenactment.

History.—s. 8, ch. 84-298; s. 1, ch. 85-301.

CHAPTER 119

PUBLIC RECORDS

119.011 Definitions.
119.07 Inspection and examination of records, exemptions.

119.011 Definitions.--For the purpose of this chapter:

(1) "Public records" means all documents, papers, letters, maps, books, tapes, photographs, films, sound recordings or other material, regardless of physical form or characteristics, made or received pursuant to law or ordinance or in connection with the transaction of official business by any agency.

(2) "Agency" means any state, county, district, authority, or municipal officer, department, division, board, bureau, commission, or other separate unit of government created or established by law and any other public or private agency, person, partnership, corporation, or business entity acting on behalf of any public agency.

(3)(a) "Criminal intelligence information" means information with respect to an identifiable person or group of persons collected by a criminal justice agency in an effort to anticipate, prevent, or monitor possible criminal activity.

(b) "Criminal investigative information" means information with respect to an identifiable person or group of persons compiled by a criminal justice agency in the course of conducting a criminal investigation of a specific act or omission, including, but not limited to, information derived from laboratory tests, reports of investigators or informants, or any type of surveillance.

(c) "Criminal intelligence information" and "criminal investigative information" shall not include:

1. The time, date, location, and nature of a reported crime.

2. The name, sex, age, and address of a person arrested or of the victim of a crime except as provided in s. 119.07(3)(h).

3. The time, date, and location of the incident and of the arrest.

4. The crime charged.

5. Documents given or required by law or agency rule to be given to the person arrested, except as provided in s. 119.07(3)(h), and, except that the court in a criminal case may order that certain information required by law or agency rule to be given to the person arrested be maintained in a confidential manner and exempt from the provisions of s. 119.07(1) until released at trial if it is found that the release of such information would:

a. Be defamatory to the good name of a victim or witness or would jeopardize the safety of such victim or witness; and

b. Impair the ability of a state attorney to locate or prosecute a codefendant.

The exemptions in this subparagraph are subject to the Open Government Sunset Review Act in accordance with s. 119.14.

6. Informations and indictments except as provided in s. 905.26.

(d) The word "active" shall have the following meaning:

1. Criminal intelligence information shall be considered "active" as long as it is related to intelligence gathering conducted with a reasonable, good faith belief that it will lead to detection of ongoing or reasonably anticipated criminal activities.

2. Criminal investigative information shall be considered "active" as long as it is related to an ongoing investigation which is continuing with a reasonable, good faith anticipation of securing an arrest or prosecution in the foreseeable future.

In addition, criminal intelligence and criminal investigative information shall be considered "active" while such information is directly related to pending prosecutions or appeals. The word "active" shall not apply to information in cases which are barred from prosecution under the provisions of s. 775.15 or other statute of limitation.

(4) "Criminal justice agency" means any law enforcement agency, court, or prosecutor. The term also includes any other agency charged by law with criminal law enforcement duties, or any agency having custody of criminal intelligence information or criminal investigative information for the purpose of assisting such law enforcement agencies in the conduct of active criminal investigation or prosecution or for the purpose of litigating civil actions under the Racketeer Influenced and Corrupt Organization Act, during the time that such agencies are in possession of criminal intelligence information or criminal investigative information pursuant to their criminal law enforcement duties.

History.--s. 1, ch. 67-125; ... s. 73-98; s. 3, ch. 75-225; ss. 1, 2, ch. 79-187; s. 8, ch. 80-531; s. 1, ch. 86-184.

Cf. ss. 895.01-895.06, Florida Racketeer Influenced and Corrupt Organization Act.

119.07 Inspection and examination of records; exemptions.--

(1)(a) Every person who has custody of a public record shall permit the record to be inspected and examined by any person desiring to do so, at any reasonable time, under reasonable conditions, and under supervision by the custodian of the public record or his designee. The custodian shall furnish a copy or a certified copy of the record upon payment of the fee prescribed by law or, if a fee is not prescribed by law, upon payment of the actual cost of duplication of the record. The phrase "actual cost of duplication" means the cost of the material and supplies used to duplicate the record, but it does not include the labor cost or overhead cost associated with such duplication. However, the charge for copies of county maps or aerial photographs supplied by county constitutional officers may also include a reasonable charge for the labor and overhead associated with its duplication. Unless otherwise provided by law, the fees to be charged for duplication of public records shall be collected, deposited, and accounted for in the manner prescribed for other operating funds of the agency.

(b) If the nature or volume of public records requested to be inspected, examined, or copied pursuant to this subsection is such as to require extensive use of information technology resources or extensive clerical or su-

pervisory assistance by personnel of the agency involved, or both, the agency may charge, in addition to the actual cost of duplication, a special service charge, which shall be reasonable and shall be based on the cost incurred for such extensive use of information technology resources or the labor cost of the personnel providing the service that is actually incurred by the agency or attributable to the agency for the clerical and supervisory assistance required, or both. "Information technology resources" shall have the same meaning as in s. 282.303(10).

(c) When ballots are produced under this section for inspection or examination, no persons other than the supervisor of elections or his employees shall touch the ballots. The supervisor of elections shall make a reasonable effort to notify all candidates by telephone or otherwise of the time and place of the inspection or examination. All such candidates, or their representatives, shall be allowed to be present during the inspection or examination.

(2)(a) A person who has custody of a public record and who asserts that an exemption provided in subsection (3) or in a general or special law applies to a particular public record or part of such record shall delete or excise from the record only that portion of the record with respect to which an exemption has been asserted and validly applies, and such person shall produce the remainder of such record for inspection and examination. If the person who has custody of a public record contends that the record or part of it is exempt from inspection and examination, he shall state the basis of the exemption which he contends is applicable to the record, including the statutory citation to an exemption created or afforded by statute, and, if requested by the person seeking the right under this subsection to inspect, examine, or copy the record, he shall state in writing and with particularity the reasons for his conclusion that the record is exempt.

(b) In any civil action in which an exemption to subsection (1) is asserted, if the exemption is alleged to exist under or by virtue of paragraph (e), paragraph (f), paragraph (g), paragraph (m), paragraph (o), or paragraph (r) of subsection (3), the public record or part thereof in question shall be submitted to the court for an inspection in camera. If an exemption is alleged to exist under or by virtue of paragraph (d) of subsection (3), an inspection in camera will be discretionary with the court. If the court finds that the asserted exemption is not applicable, it shall order the public record or part thereof in question to be immediately produced for inspection, examination, or copying as requested by the person seeking such access.

(c) Even if an assertion is made by the custodian of a public record that a requested record is not a public record subject to public inspection and examination under subsection (1), the requested record shall, nevertheless, not be disposed of for a period of 30 days after the date on which a written request requesting the right to inspect, examine, or copy the record was served on or otherwise made to the custodian of the record by the person seeking access to the record. If a civil action is instituted within the 30-day period to enforce the provisions of this section with respect to the requested record, the custodian shall not dispose of the record except by order of a court of competent jurisdiction after notice to all affected parties.

(d) The absence of a civil action instituted for the purpose stated in paragraph (c) will not relieve the custodian of his duty to maintain the record as a public record if the record is in fact a public record subject to public inspection and examination under subsection (1) and will not otherwise excuse or exonerate the custodian from any unauthorized or unlawful disposition of such record.

(3)(a) All public records which are presently provided by law to be confidential or which are prohibited from being inspected by the public, whether by general or special law, are exempt from the provisions of subsection (1).

(b) All public records referred to in ss. 199.222, 228.093, 257.261, 288.075, 624.319(3) and (4), and 655.057(1)(b), (3), and (4) are exempt from the provisions of subsection (1).

(c) Examination questions and answer sheets of examinations administered by a governmental agency for the purpose of licensure, certification, or employment are exempt from the provisions of subsection (1). A person who has taken such an examination shall have the right to review his own completed examination.

(d) Active criminal intelligence information and active criminal investigative information are exempt from the provisions of subsection (1).

(e) Any information revealing the identity of a confidential informant or a confidential source is exempt from the provisions of subsection (1).

(f) Any information revealing surveillance techniques or procedures or personnel is exempt from the provisions of subsection (1). Notwithstanding s. 119.14, any comprehensive inventory of state and local law enforcement resources compiled pursuant to part I, chapter 23, and any comprehensive policies or plans compiled by a criminal justice agency pertaining to the mobilization, deployment, or tactical operations involved in responding to emergencies, as defined in s. 252.34(2), are exempt from the provisions of subsection (1) and unavailable for inspection, except by personnel authorized by a state or local law enforcement agency, the office of the Governor, the Department of Legal Affairs, the Department of Law Enforcement, or the Department of Community Affairs as having an official need for access to the inventory or comprehensive policies or plans. This exemption is subject to the Open Government Sunset Review Act in accordance with s. 119.14.

(g) Any information revealing undercover personnel of any criminal justice agency is exempt from the provisions of subsection (1).

(h) Any criminal intelligence information or criminal investigative information including the photograph, name, address, or other fact or information which reveals the identity of the victim of the crime of sexual battery as defined in chapter 794, the identity of the victim of the crime of lewd, lascivious, or indecent assault upon or in the presence of a child, as defined in chapter 800, or the identity of the victim of the crime of child abuse as defined by chapter 827 and any criminal intelligence information or criminal investigative information or other

criminal record, including those portions of court records, which may reveal the identity of a person who is a victim of any sexual offense, including a sexual offense proscribed in chapter 794, chapter 800, or chapter 827, is exempt from the provisions of subsection (1).

(i) Any criminal intelligence information or criminal investigative information which reveals the personal assets of the victim of a crime, other than property stolen or destroyed during the commission of the crime, is exempt from the provisions of subsection (1).

(j) All criminal intelligence and criminal investigative information received by a criminal justice agency prior to January 25, 1979, is exempt from the provisions of subsection (1).

(k) The home addresses, telephone numbers, and photographs of active or former law enforcement personnel; the home addresses, telephone numbers, photographs, and places of employment of the spouses and children of active or former law enforcement personnel; and the names and locations of schools attended by the children of active or former law enforcement personnel are exempt from the provisions of subsection (1).

(l) Any information provided to an agency of state government or to an agency of a political subdivision of the state for the purpose of forming ridesharing arrangements, which information reveals the identity of an individual who has provided his name for ridesharing arrangements as defined in s. 341.031(6), is exempt from the provisions of subsection (1).

(m) Any information revealing the substance of a confession of a person arrested is exempt from the provisions of subsection (1), until such time as the criminal case is finally determined by adjudication, dismissal, or other final disposition.

(n) A patient record obtained by the Hospital Cost Containment Board established under s. 395.503, which record contains the name, residence or business address, telephone number, social security or other identifying number, or photograph of any person or the spouse, relative, or guardian of such person or which record is patient-specific or otherwise identifies the patient, either directly or indirectly, is exempt from the provisions of paragraph (1)(a).

(o) A public record which was prepared by an agency attorney (including an attorney employed or retained by the agency or employed or retained by another public officer or agency to protect or represent the interests of the agency having custody of the record) or prepared at the attorney's express direction, which reflects a mental impression, conclusion, litigation strategy, or legal theory of the attorney or the agency, and which was prepared exclusively for civil or criminal litigation or for adversarial administrative proceedings, or which was prepared in anticipation of imminent civil or criminal litigation or imminent adversarial administrative proceedings, is exempt from the provisions of subsection (1) until the conclusion of the litigation or adversarial administrative proceedings. When asserting the right to withhold a public record pursuant to this paragraph, the agency shall identify the potential parties to any such criminal or civil litigation or adversarial administrative proceedings. If a court finds that the document or other record has been improperly withheld under this paragraph, the party seeking access to such document or record shall be awarded reasonable attorney's fees and costs in addition to any other remedy ordered by the court.

(p) Sealed bids or proposals received by an agency pursuant to invitations to bid or requests for proposals are exempt from the provisions of subsection (1) until such time as the agency provides notice of a decision or intended decision pursuant to s. 120.53(5)(a) or within 10 days after bid or proposal opening, whichever is earlier.

(q) In any case in which an agency of the executive branch of state government seeks to acquire real property by purchase or through the exercise of the power of eminent domain all appraisals, other reports relating to value, offers, and counteroffers must be in writing and are exempt from the provisions of s. 119.01 and subsection (1) until execution of a valid option contract or a written offer to sell which has been conditionally accepted by the agency, at which time the exemption shall expire. The agency shall not finally accept the offer for a period of 30 days in order to allow public review of the transaction. The agency may give conditional acceptance to any option or offer subject only to final acceptance by the agency after the 30-day review period. If a valid option contract is not executed, or if a written offer to sell is not conditionally accepted by the agency, then the exemption from the provisions of this chapter shall expire at the conclusion of the condemnation litigation of the subject property. Nothing in this section shall be construed to provide an exemption from or exception to s. 286.011. For the purpose of this paragraph "option contract" means an agreement of an agency of the executive branch of state government to purchase real property subject to final agency approval. This paragraph shall have no application to other exemptions from the requirements of s. 119.01 or subsection (1) which are contained in other provisions of law and shall not be construed to be an express or implied repeal thereof.

(r) Data processing software obtained by an agency under a licensing agreement which prohibits its disclosure and which software is a trade secret, as defined in s. 812.081, and agency-produced data processing software which is sensitive are exempt from the provisions of subsection (1). The designation of agency-produced software as sensitive shall not prohibit an agency head from sharing or exchanging such software with another public agency. As used in this paragraph:

1. "Data processing software" has the same meaning as in ²s. 282.303(6).

2. "Sensitive" means only those portions of data processing software, including the specifications and documentation, used to:

a. Collect, process, store, and retrieve information which is exempt from the provisions of subsection (1);

b. Collect, process, store, and retrieve financial management information of the agency, such as payroll and accounting records; or

c. Control and direct access authorizations and security measures for automated systems.

(s) The names, addresses, and amounts contributed by donors to the state Fine Arts Endowment Program or to a local organization's fine arts endowment program

fund created pursuant to s. 265.606 shall, at the request of the donor, be exempt from the provisions of subsection (1).

(t) A patient record obtained by the Department of Health and Rehabilitative Services pursuant to s. 641.27 from a health maintenance organization or from a provider of a health maintenance organization as to subscribers treated by the provider pursuant to a provider contract with a health maintenance organization, which record contains the name, the residential or business address, the telephone, social security, or other identifying number, or a photograph of any subscriber or of the spouse, relative, or guardian of the subscriber, or which record is patient-specific or otherwise identifies the patient, either directly or indirectly, is exempt from the provisions of subsection (1).

(u) A report obtained by the Department of Insurance from a health maintenance organization pursuant to s. 641.311, to the extent that such report contains the name, the residential or business address, the telephone, social security, or other identifying number, or a photograph of any subscriber or of the spouse, relative, or guardian of the subscriber, or other subscriber-identifying information, is exempt from the provisions of subsection (1).

(v) All complaints and other records in the custody of any unit of local government which relate to a complaint of discrimination relating to race, color, religion, sex, national origin, age, handicap, marital status, sale or rental of housing, the provision of brokerage services, or the financing of housing shall be exempt from the provisions of subsection (1) until a finding is made relating to probable cause, the investigation of the complaint becomes inactive, or the complaint or other record is made part of the official record of any hearing or court proceeding. This provision shall not affect any function or activity of the Florida Commission on Human Relations. Any state or federal agency which is authorized to have access to such complaints or records by any provision of law shall be granted such access in the furtherance of such agency's statutory duties, notwithstanding the provisions of this section. This paragraph shall not be construed to modify or repeal any special or local act. *This exemption is subject to the Open Government Sunset Review Act in accordance with s. 119.14.

(w) All complaints and other records in the custody of any agency in the executive branch of state government which relate to a complaint of discrimination relating to race, color, religion, sex, national origin, age, handicap, or marital status in connection with hiring practices, position classifications, salary, benefits, discipline, discharge, employee performance, evaluation, or other related activities shall be exempt from the provisions of subsection (1) until a finding is made relating to probable cause, the investigation of the complaint becomes inactive, or the complaint or other record is made part of the official record of any hearing or court proceeding. This provision shall not affect any function or activity of the Florida Commission on Human Relations. Any state or federal agency which is authorized to have access to such complaints or records by any provision of law shall be granted such access in the furtherance of such agency's statutory duties, notwithstanding the provisions of this section. This exemption is subject to the Open Government Sunset Review Act in accordance with s. 119.14.

(x) A patient record obtained from a hospital by the Department of Health and Rehabilitative Services or its agent pursuant to s. 395.031, which record contains the name, residence or business address, telephone number, social security or other identifying number, or photograph of any person or the spouse, relative, or guardian of such person or which record is patient-specific or otherwise identifies the patient, either directly or indirectly, is exempt from the provisions of subsection (1).

(y) All records supplied by a telecommunications company to a state or local governmental agency which contain the name, address, and telephone number of subscribers are exempt from the provisions of subsection (1).

(4) Nothing in this section shall be construed to exempt from subsection (1) a public record which was made a part of a court file and which is not specifically closed by order of court, except as provided in paragraphs (e), (f), (g), (m), (o), and (r) of subsection (3) and except information or records which may reveal the identity of a person who is a victim of a sexual offense as provided in paragraph (h) of subsection (3).

(5) Nothing in subsection (3) shall be interpreted as providing an exemption from or exception to s. 286.011.

(6) The provisions of this section are not intended to expand or limit the provisions of Rule 3.220, Florida Rules of Criminal Procedure, regarding the right and extent of discovery by the state or by a defendant in a criminal prosecution.

History.—s. 7, ch. 67-125; s. 4, ch. 75-225; s. 2, ch. 77-60; s. 2, ch. 77-75; s. 2, ch. 77-94; s. 2, ch. 77-156; s. 2, ch. 78-81; ss. 2, 4, 6, ch. 79-187; s. 2, ch. 80-273; s. 1, ch. 81-245; s. 1, ch. 82-95; s. 36, ch. 82-243; s. 8, ch. 83-215; s. 2, ch. 83-269; s. 1, ch. 83-286; s. 5, ch. 84-252; s. 1, ch. 85-18; s. 1, ch. 85-45; s. 1, ch. 85-73; s. 1, ch. 85-86; s. 7, ch. 85-152; s. 1, ch. 85-177; s. 4, ch. 85-301; s. 2, ch. 86-11; s. 1, ch. 86-21; s. 1, ch. 86-109; s. 2, ch. 87-399; s. 2, ch. 88-188; s. 1, ch. 88-384.

*Note.—The reference to "s. 282.303(10)" was substituted by the editors for a reference to "s. 282.303(9)," to conform to the renumbering by s. 17, ch. 87-137.

*Note.—The reference to "s. 282.303(6)" was substituted by the editors for a reference to "s. 282.303(5)," to conform to the renumbering by s. 17, ch. 87-137.

Note.—Additional exemptions from the application of this section are indexed in Volume 4 of this edition in the General Index under the heading "Public Records."

CHAPTER 120

ADMINISTRATIVE PROCEDURE ACT

120.52 Definitions.
120.53 Adoption of rules of procedure and public inspection.
120.575 Taxpayer contest proceedings.
120.65 Hearing officers.

120.52 Definitions.—As used in this act:

(1) "Agency" means:

(a) The Governor in the exercise of all executive powers other than those derived from the constitution.

(b) Each other state officer and each state department, departmental unit described in s. 20.04, commission, regional planning agency, board, district, and authority, including, but not limited to, those described in chapters 163, 298, 373, 380, and 582 and s. 186.504, ex-

My research has not revealed any statutory requirement that a sound recording be made of such meetings. Attorney General Opinion 86-21 (s. 286.011 does not require meetings of board of commissioners of drainage district to be tape recorded); ss. 286.011 and 230.23, F.S. However, notwithstanding the lack of a statutory requirement that such a recording be made, for the following reasons, it is my opinion that once made, such materials are subject to the requirements of ch. 119, F.S., Florida's Public Records Law. Such (sound) tape recordings fall within the definition of "public records" pursuant to the express provisions of s. 119.011(1), which defines that term as:

> [A]ll documents, papers, letters, maps, books, tapes, photographs, films, *sound recordings* or other material, regardless of physical form or characteristics, *made* or received pursuant to law or ordinance or *in connection with the transaction of official business by any agency.* (Emphasis supplied.)

The term "agency," as used in s. 119.011(1), F.S., includes school districts. *See* s. 119.011(2), F.S. Thus the recordings described above are subject to the requirements of ch. 119, specifically s. 119.07, F.S., which requires custodians of public records to allow inspection and examination of public records by any person desiring to do so, at any reasonable time, under reasonable conditions, and under supervision by the custodian of the public record or his designee, and to furnish copies of such records upon payment of the fee prescribed by law or if none is prescribed, upon payment of the actual cost of duplication.

Regarding disposal of these tapes, *see* s. 119.041, F.S., as amended by s. 5, ch. 86-163, Laws of Florida, which provides for the systematic disposal of records no longer needed subject to the consent of the records and information management services of the Department of State in accordance with s. 257.36; and s. 257.36(7), F.S., as amended by s. 46, ch. 86-163, Laws of Florida, providing that no record shall be destroyed or disposed of by any agency unless approval of the division is first obtained and requiring the division to adopt reasonable binding rules relating to the destruction and disposal of records. *See also* AGO's 86-21, 82-47, 81-12 and 75-45. Paragraph (a) of s. 257.36(7), as amended by s. 46 of ch. 86-163, Laws of Florida, requires the division's rules to contain procedures for disposal. Thus, it would appear that the disposal of the above described tape recordings would be controlled by schedules referred to in s. 257.36(7)(a), F.S., as amended.

AGO 86-94—October 28, 1986

CIRCUIT COURT CLERKS

COPYRIGHT OF COMPUTER PROGRAMS UNAUTHORIZED

To: Charlie Green, Clerk of Courts, Lee County

Prepared by: Craig Willis, Assistant Attorney General

QUESTIONS:

1. May the clerk of the circuit court copyright computer programs for certain financial and accounting functions?

2. If the clerk is authorized to copyright such programs, may he charge other clerks or other public agencies a fee for such programs in order to recover the expense incurred in developing them?

SUMMARY:

Unless legislatively or judicially determined otherwise, the clerk of the circuit court does not have the authority to copyright computer programs for certain financial and accounting functions developed by his staff.

You state in your letter of inquiry that in connection with the performance of the duties and responsibilities of the Office of Clerk of the Circuit Court, your staff has developed certain computer programs for certain financial and accounting functions. You further state that clerks from other counties and other agencies have inquired of your office whether they may obtain these programs for their own use. Thus, you wish to know if you have the authority to copyright these programs in order to prevent their unauthorized use, and if so, charge other clerks and other public agencies a fee for such programs in order to recover the expense incurred in developing them.

The clerk of the circuit court is a county officer, and, unless otherwise provided by county charter or special law approved by vote of the electors, the *ex officio* clerk of the board of county commissioners, county auditor, county recorder, and custodian of county funds, whose powers and duties in any of his several capacities are fixed by law. *See* s. 5(c), Art. II, and s. 1(d), Art. VIII, State Const.; *see also* s. 16, Art. V, State Const., and Alachua County v. Powers, 351 So.2d 32, 35 (Fla. 1977). While the clerk of the court derives his authority and responsibility from both constitutional and statutory provisions, Alachua County v. Powers, *supra* at 35, the clerk's powers, as those of other constitutional county officers, are limited to those which have been expressly provided or are clearly necessary to give meaning and effect to those which have been expressly granted. Security Finance Company v. Gentry, 109 So. 220 (Fla. 1926). *See, e.g.*, AGO's 78-56 and 75-161; and Edgerton v. International Company, 89 So.2d 488 (Fla. 1956). *And see* Overholser v. Overstreet, 383 So.2d 953 (3 D.C.A. Fla., 1980) (clerk's authority is entirely statutory, and his official action to be binding upon others, must be in conformity with such statutes); Ferlita v. State, 380 So.2d 1118 (2 D.C.A. Fla., 1980) (clerk of court's power to act must clearly appear from particular statute). Further, if any doubt exists as to the existence of authority, it should not be assumed. Gessner v. Del-Air Corporation, 17 So.2d 522 (Fla. 1944).

Chapter 28, F.S., which sets forth the powers and duties of the clerks of the circuit court, contains no provision authorizing or relating to the copyrighting of computer programs developed by the clerk or his staff. No other general or special law expressly authorizing such copyrighting by the clerk has been brought to the attention of this office. *Compare, e.g.*, s. 240.229, F.S., authorizing each university to perform all things necessary to secure letters of patent, copyrights, and trademarks on any work products and to enforce its rights therein. Nor can I conclude that such copyrighting is essential to or necessary for the implementation of any other express duty and responsibility of the clerk. *See generally* Florida State University v. Jenkins, 323 So.2d 597 (1 D.C.A. Fla., 1975) (power to be implied must be essential in order to carry out expressly granted power or duty imposed); Haines City v. Certain Lands, Etc., 178 So. 143 (Fla. 1937) (power sought to be implied from express grant of power must be necessary, indispensable or essential, not merely convenient to the attainment of the declared objects and purposes); Southern Utilities Company v. City of Palatka, 99 So. 236 (Fla. 1923). You ask whether the right to copyright is vested solely with the Department of State pursuant to ss. 286.021 and 286.031, F.S. Section 286.021 in part provides that the legal title to any copyright now owned or held, or as may be hereafter be acquired, owned or held by the *state*, or any of its boards, commissions or agencies is granted to and vested in the Department of State. Section 286.031 provides that the department is authorized to secure copyrights and to take any and all action necessary to protect the same against improper or unlawful use of infringement. These provisions

of law relate to the department's function to secure, hold and protect copyrights for the state and its boards, commissions or agencies. While the several counties are political subdivisions of the state and are sometimes referred to as agencies of the state, they are separate and distinguishable local governmental units that have no inherent power, but derive their powers from the sovereign state and operate independently thereof. *See* Amos v. Mathews, 126 So. 308 (Fla. 1930). When the Legislature intends to include counties within the ambit of a statute, express inclusion is usually made or their inclusion as political subdivisions of the state is made. *See, e.g.*, ss. 119.011(2), 120.52(1), 121.021(10), 206.022(2), 218.31(1), and 219.01(1), F.S. *And see* ch. 20, F.S., setting forth the organizational structure of state government. Powers delegated to the Department of State pertaining to the state and its boards, commissions or agencies by the State Legislature therefore would not appear to be relevant to the issues presented herein.

Chapter 119, F.S., Florida's Public Records Law, makes all public records made or received pursuant to law or ordinance or in connection with the transaction of official business by any public agency open for inspection by any person. Sections 119.01 and 119.07, F.S., as amended by chs. 86-11, 86-21, 86-109 and 86-163, Laws of Florida. The custodian of the public record in question must furnish a copy of the record upon demand and payment of the fee prescribed by law or, if no fee is prescribed, upon payment of the actual cost of duplication. The actual cost of duplication is defined to mean "the cost of the material and supplies used to duplicate the record, but . . . [not] the labor cost or overhead cost associated with such duplication." Section 119.07(1)(a), F.S. The term "public records" is defined by s. 119.011(1), F.S., to mean:

> [A]ll documents, papers, letters, maps, books, tapes, photographs, films, sound recordings or other material, regardless of physical form or characteristics, made or received pursuant to law or ordinance or in connection with the transaction of official business by any agency.

See also Shevin v. Byron, Harless, Schaffer, Reid and Associates, Inc., 379 So.2d 633, 640 (Fla. 1980), stating that for purposes of ch. 119, a "public record" is "any material prepared in connection with official agency business which is intended to perpetuate, communicate, or formalize knowledge of some type. . . ." *And see* Seigle v. Barry, 422 So.2d 63 (4 D.C.A. Fla., 1982), *petition for review denied*, 431 So.2d 988 (Fla. 1983). Thus, it is clear that a computer program developed by a public agency in order to perform certain financial and accounting functions is a public record for purposes of ch. 119, as amended. Further, I am not aware of, nor has my attention been drawn to, a statute authorizing the clerk to charge and collect a fee from persons seeking access to computer stored information in order to recoup the costs associated with developing the agency's program. *Compare* s. 119.085, F.S., authorizing a custodian to charge a fee for remote electronic access to public records.

In regard to any exemption of such records from the requirements of ch. 119, F.S., as amended, the Florida Supreme Court in Wait v. Florida Power and Light Company, 372 So.2d 420, 425 (Fla. 1979), held that "only those public records that are provided by statutory law to be confidential or which are expressly exempted by general or special law" are exempt from public disclosure and copying. As you point out in your letter s. 119.07(3)(r)2., F.S., provides an exemption for certain sensitive agency-produced data processing software. That exemption provides that:

> "Sensitive" means only those portions of data processing software, including the specifications and documentation, used to:
> a. Collect, process, store, and retrieve information which is exempt from the provisions of subsection (1);

b. Collect, process, store, and retrieve financial management information of the agency, such as payroll and accounting records; or
c. Control and direct access authorizations and security measures for automated systems.

However, the fact that a particular computer program may be classified as "sensitive" under this exemption from the disclosure and copying requirements of subsection (1), in no way provides any authorization, express or implied, for the public agency to acquire a copyright for the programs in question.

The answer to your first question makes it unnecessary to answer your second question.

DEPARTMENT OF LEGAL AFFAIRS
OFFICE OF THE ATTORNEY GENERAL
THE CAPITOL
TALLAHASSEE, FLORIDA 32301

JIM SMITH
Attorney General
State of Florida

January 2, 1987

INFORMATION COPY

87-1

The Honorable Freda Wright
Clerk, Circuit Court and Recorder
Indian River County
Post Office Box 1028
Vero Beach, Florida 32961-1028

Re: RECORDS--CLERKS, CIRCUIT COURTS--no authority to charge additional fees for in-house produced computer programs. s. 119.07(1), F.S.

Dear Ms. Wright:

This is in response to your request for an opinion on substantially the following question:

> MAY THE CLERK OF THE COURT IN PROVIDING COPIES OF COMPUTER SOFTWARE PROGRAMS PRODUCED BY THAT OFFICE RECOUP SOME OF THE IN-HOUSE COSTS INVOLVED IN WRITING SUCH COMPUTER PROGRAMS?

In AGO 86-94, this office was faced with the question of whether the clerk of the circuit court could copyright computer programs which had been developed by office staff for certain financial and accounting functions. That opinion concluded that the clerk does not have the authority to copyright such computer programs. This office further concluded, in AGO 86-94, that the computer programs were subject to Florida's Public Records Law, Ch. 119, F.S., and must be disclosed and permitted to be copied unless such program could be classified as "sensitive agency-produced data processing software." See, s. 119.07(3)(r), F.S. You query in general whether computer programs produced by local governments are considered in the public domain and must be made available to other units of local government on a no-charge basis. This office, as a matter of authority and policy, can only comment on the clerk's power and duties and responsibilities, and not on the authority and duties and responsibilities of other public officers not presently seeking the opinion of the Attorney General. You wish to know whether your office may recoup some of the in-house costs involved in developing the agency's program. Applying pertinent rules of law

applicable the clerk, I am constrained to conclude, unless and until legislatively provided otherwise, that you have no authority to recoup such costs.

The clerk of the circuit court is a county officer whose powers, duties and responsibilities are fixed by law. See, s. 5(c), Art. II, and s. 1(d), Art. VIII, State Const.; Alachua County v. Powers, 351 So.2d 32, 35 (Fla. 1977). The clerk's authority and power is limited to that which is expressly provided by law, or which is clearly necessary to give meaning and effect to such duties and responsibilities which have been expressly granted. See, Overholser v. Overstreet, 383 So.2d 953 (3 D.C.A. Fla., 1980) (clerk's authority is entirely statutory, and his official action to be binding upon others, must be in conformity with such statutes); Ferlita v. State, 380 So.2d 1118 (2 D.C.A. Fla., 1980) (clerk of court's power to act must clearly appear from particular statute). See also, AGO's 86-94, 78-95 and 75-161. If there is any doubt as to the existence of authority to do a particular thing, it should not be assumed. Gessner v. Del-Air Corporation, 17 So.2d 522 (Fla. 1944).

As stated above, this office in AGO 86-94 concluded that computer software programs developed by a public agency were subject to the Public Records Law, Ch. 119, F.S. Section 119.07(1)(a), F.S., requires the custodian of public records to furnish a copy or a certified copy of the record upon payment of the fee prescribed by law or, if a fee is not prescribed by law, upon payment of the actual cost of duplication. That provision defines the phrase "actual cost of duplication" to mean "the cost of the material and supplies used to duplicate the record, but . . . [not] the labor cost or overhead cost associated with such duplication." And see, s. 119.07(1)(b), F.S., which provides that if the nature or volume of public records requested to be inspected, examined, or copied is such as to require extensive use of information technology resources or extensive clerical or supervisory assistance by personnel of the agency involved, or both, the agency may charge, in addition to the actual cost of duplication, a special service charge based upon the cost incurred for such extensive use of information technology resources or the labor cost of the personnel providing the service. The general laws pertaining to the clerks of the circuit court, contained in Ch. 28, F.S., setting forth the powers and duties of the office, contain no provision authorizing the clerk to charge a fee for providing a copy of computer software in order to recoup the costs involved in developing the program. Nor has any other general or special law expressly authorizing such charge been brought to the attention of this

office. Cf., s. 28.24, F.S., prescribing service charges the clerk shall make for providing enumerated services and copies. A service charge for providing copies of in-house computer programs are not among the enumerated matter. See also, AGO 85-80 concluding that service charges enumerated in s. 28.24(8)(a) are not applicable to such unrecorded documents as the minutes of public meetings, resolutions or budgets which may be in the custody of the clerk of the circuit court as ex officio clerk of the board of county commissioners. The rule of construction, expressio unius est exclusio alterius, the express mention of one thing implies the exclusion of other things not mentioned would apply to this situation. See, Dobbs v. Sea Isle Hotel, 56 So.2d 341 (Fla. 1952); Ideal Farms Drainage District v. Certain Lands, 19 So.2d 234 (Fla. 1944); Devin v. City of Hollywood, 351 So.2d 1022 (4 D.C.A. Fla., 1976). In the absence of a statute specifying a fee which may be charged and except as provided in s. 119.07(1), F.S., there is no authority for the clerk to recoup in-house costs for writing computer programs.

I am therefore of the opinion that, unless and until legislatively amended otherwise, the clerk of the circuit court does not have the authority to charge a fee, other than the actual cost of making the copy, for providing copies of computer software programs in order to recoup the costs associated with writing such programs.

Sincerely,

JIM SMITH
ATTORNEY GENERAL

Prepared by:

Craig Willis
Assistant Attorney General

JS/CW/gk

ROBERT A. BUTTERWORTH
Attorney General
State of Florida

OFFICE OF THE ATTORNEY GENERAL

DEPARTMENT OF LEGAL AFFAIRS
THE CAPITOL
TALLAHASSEE, FLORIDA 32399-1050

INFORMATION COPY

June 1, 1988

88-23

The Honorable Janet Reno
State Attorney
Metropolitan Dade County
Justice Building
1351 Northwest 12th Street
Miami, Florida 33125

Dear Ms. Reno:

You have asked substantially the following questions:

(1) Are videotapes produced by the state attorney's office of training sessions conducted for the benefit of the staff of that office public records subject to disclosure?

(2) If so, what fees may be charged for viewing and/or copying?

In sum, I am of the opinion that:

(1) Videotapes produced by the state attorney's office of training sessions are public records and are subject to disclosure in the absence of a statute making the information contained therein confidential.

(2) In the absence of a statute specifically authorizing a state attorney to recoup the costs of producing the training program, a state attorney is not authorized to recoup such costs. In the absence of a statute providing otherwise, the only fees that may be imposed are those authorized in s. 119.07(1), F.S.

According to your letter, your office recently began conducting programs that will be certified by The Florida Bar pursuant to the new continuing legal education rule. These programs are

AN AFFIRMATIVE ACTION/EQUAL OPPORTUNITY EMPLOYER

being videotaped for later viewing by the assistant state attorneys. Your office has apparently received a request from a private attorney to view one of the videotapes so that he may obtain credit pursuant to the continuing legal education rule.[1]

You state that: (1) there may be contractual or copyright restrictions against such access; (2) the tapes may contain information dealing with prosecutorial tactics or sensitive topics; and (3) it may be impractical to provide these facilities.

QUESTION ONE

Chapter 119, F.S., the Florida Public Records Law, makes all records made or received pursuant to law or ordinance or in connection with the transaction of official business by any agency open for inspection by any person[2] The term "public record" is broadly defined and encompasses "documents, papers, letters, maps, books, tapes, photographs, films, sound recordings or other material, regardless of physical form or characteristics . . . ."[3] (e.s.)

It is clear that videotapes made by the state attorney's office of that office's training programs are public records for purposes of Ch. 119, F.S. I am not aware of, nor have you brought to my attention, any statute which would generally exempt videotapes produced by the state attorney's office from the disclosure provisions of s. 119.07, F.S.[4] As stated by The Supreme Court of Florida in Wait v. Florida Power and Light Company,[5] "only those public records that are provided by statutory law to be confidential or which are expressly exempted by general or special law" are exempt from public disclosure and copying.

You specifically ask whether the videotapes are public records "irrespective of any contractual or copyright limitations." This office has previously considered the authority of a public officer to obtain a copyright of material produced by his office in connection with the transaction of official business. In AGO 86-94, this office concluded that in the absence of specific statutory authorization, the clerk of the circuit court was not authorized to copyright computer programs for certain financial and accounting functions.

I am not aware of any statute which authorizes the state attorney to copyright materials prepared by his office.[6] Nor can I conclude that copyrighting such videotapes is essential to, or necessary for, the implementation of an express power or duty of the state attorney.[7]

In the absence of a statute authorizing the state attorney to copyright material produced by his office, I am of the opinion that a state attorney does not possess such authority. To the extent that the state attorney's office may receive copyrighted work in connection with its official business, the federal statute placing limitations on the reproduction of copyrighted material will control.[8] However, as this office noted in AGO 82-63, there is a distinction between the examination and the copying of copyrighted material. Thus, this office stated:

> In short, agencies should not reproduce, or permit the reproduction of, or distribute copies of, copyrighted work to the public but may permit the public access to copyrighted work in their possession for examination and inspection purposes only.

Moreover, s. 119.011(2), F.S., in defining "Agency" for purposes of Ch. 119, F.S., includes "any other public or private agency, person, partnership, corporation, or business entity acting on behalf of any public agency." Thus a public agency cannot avoid compliance with the public records law by delegating its duties and responsibilities to private persons or corporations.[9]

Therefore, it is my opinion that the videotapes made by the state attorney's office of its training sessions are public records and are subject to disclosure in the absence of a specific statutory exemption.

QUESTION TWO

You inquire what fees may be imposed for providing access to the videotapes and whether such charges may include part of your original cost in producing the training session.

In the absence of a specific statute to the contrary, public records must be open for public inspection without charge. While s. 119.07(1)(a), F.S., authorizes the custodian of public

records to charge a fee for furnishing copies of records based upon the actual cost of duplication,[10] there is no statute which generally authorizes the imposition of a fee for the mere inspection of public records.

Section 119.07(1)(b), F.S., however, authorizes the imposition of a special service charge when the nature or volume of public records requested to be inspected or copied is such as to require extensive use of information technology resources or extensive clerical or supervisory assistance, or both. This charge shall be reasonable and shall be based upon the cost incurred for such extensive use of the information technology resources or the labor cost of the personnel providing the service that is actually incurred by the agency.

"Information technology resources" is defined as data processing hardware and software and services, supplies, personnel, facility resources, maintenance, and training.[11] A videotape and machine to view such tape would not appear to fall within the term "information technology resources" for purposes of s. 119.07(1)(b), F.S. Whether the nature or volume of the records requested to be inspected or copied is such as to require extensive clerical or supervisory assistance is a determination which must be made on a case-by-case basis. However, as this office stated in AGO 86-69, the special service charge may not be routinely imposed.

In AGO 75-50, this office considered whether a custodian could impose a fee for listening to tapes of city commission meetings. This office concluded that the fact that commission meetings were taped as opposed to stenographically recorded and, therefore, required the use of tape recorder in order to listen to such meeting, was irrelevant insofar as the imposition of a fee was concerned.

Similarly, the fact that the public record is a videotape rather than a printed document would appear to be irrelevant with respect to the imposition of a fee. Only those fees or charges which are authorized by statute may be imposed upon an individual seeking access to public records.

You ask whether you may impose a charge to recover part of the costs incurred by your office in producing the training session. In AGO 87-1, this office considered whether the clerk of the

court, in providing copies of computer software programs produced by that office, could recoup some of the in-house costs involved in writing the computer program. In the absence of a statute specifying a fee which may be charged and except as provided in s. 119.07(1), F.S., this office concluded that there was no authority for the clerk to recoup such costs.

Similarly, in the absence of a statute specifically authorizing your office to impose a fee for inspection and/or copying to recoup part of your original cost of producing the training session and except as provided in s. 119.07(1), F.S., I am of the opinion that you may not impose a fee for inspection or copying a videotape of your training programs.

Sincerely,

Robert A. Butterworth
Attorney General

RAB/tjw

---

[1] This office is without the authority to determine whether the viewing of any such tapes would satisfy the continuing legal education requirements imposed on members of The Florida Bar. Such a determination must be resolved by The Florida Bar and not by this office.

[2] Sections 119.01 and 119.07(1), F.S. And see, Shevin v. Byron, Harless, Schaffer, Reid and Associates, Inc., 379 So.2d 633, 640 (Fla. 1980), stating that for purposes of Ch. 119, F.S., a "public record" is "any material prepared in connection with official agency business which is intended to perpetuate, communicate, or formalize knowledge of some type. . . ."

[3] Section 119.011(1), F.S. And see, s. 119.011(2), F.S., defining "Agency" to mean:

> [A]ny state, county, district, authority, or municipal officer, department, division, board, bureau, commission, or other separate unit of

government created or established by law and any other public or private agency, person, partnership, corporation, or business entity acting on behalf of any public agency.

[4] Compare, s. 119.0115, F.S., exempting any videotape or video signal which, under an agreement with an agency, is produced, made, or received by, or is in the custody of, a federally licensed radio or television station or its agent is exempt from Ch. 119, F.S.; and s. 119.07(3)(r), F.S., containing a limited exemption for data processing software.

[5] 372 So.2d 420, 425 (Fla. 1979).

[6] Cf., 67 C.J.S. Officers s. 190 (powers and authority of public officers are usually fixed and determined by law; they have only such power and authority as are clearly conferred or necessarily implied from the powers granted); Lang v. Walker, 35 So. 78, 80 (Fla. 1903). And see, AGO 78-67 concluding that the authority to contract did not grant the board of trustees of a community college the authority to enter into a contract for the purchase of an exclusive copyright license and the right to use, distribute, and sell a videotape educational series.

Pursuant to s. 286.021, F.S., legal title to any copyright now owned or held, or as may be hereafter acquired, owned or held by the state, or any of its boards, commissions or agencies, is granted to and vested in the Department of State. And see, s. 286.031, F.S., which provides that the Department of State is hereby authorized to secure copyrights and to take any and all action necessary to protect such copyrights against improper or unlawful use of infringement. Compare, s. 24.105(12), F.S., authorizing the Department of Lottery to hold copyrights.

[7] See generally, Florida State University v. Jenkins, 323 So.2d 597 (1 D.C.A. Fla., 1975) (power to be implied from express power must be essential in order to carry out expressly granted power or duty imposed); Haines City v. Certain Lands, Etc., 178 So. 143 (Fla. 1937) (power sought to be implied from express power must be necessary, indispensable or essential, not merely convenient to the attainment of the declared objects and purposes).

[8] Pursuant to Art. VI, U.S. Const., the Supremacy Clause, federal law will prevail over state law to the extent of any conflict. And see generally, 17 U.S.C. s. 101 et seq., the federal copyright laws.

[9] See, Shevin v. Byron, Harless, Schaffer, Reid and Associates, Inc., supra; Schwartzman v. Merritt Island Volunteer Fire Department, 352 So.2d 1230 (4 D.C.A. Fla., 1977), in which the courts found that private organizations were acting on behalf of a public agency and thus subject to Ch. 119, F.S. Compare, Parsons & Whittemore, Inc. v. Metropolitan Dade County, 429 So.2d 343 (3 D.C.A. Fla., 1983). And see, s. 287.058(1)(c), F.S., stating that every procurement for contracted services by a state agency shall be evidenced by a written agreement which shall include a provision allowing unilateral cancellation by the agency for refusal by the contractor to allow public access to materials subject to Ch. 119, F.S., and made or received by the contractor in conjunction with the contract.

[10] Section 119.07(1)(a), F.S., defines the phrase "actual cost of duplication" as "the cost of the material and supplies used to duplicate the record, but it does not include the labor cost or overhead cost associated with such duplication. . . ."

[11] Section 282.303(10), F.S. Pursuant to s. 119.07(1)(b), F.S., "information technology resources" shall have the same meaning as in s. 282.303(10), F.S.

MEMORANDUM

103.01-14

TO Manuel Garcia
O.C.S.I.S.

DATE October 7, 1987

SUBJECT Licensing Agreement for County-Generated Software Products

FROM Jay W. Williams
Assistant County Attorney

In response to your request for a legal opinion, I state that I am unaware of any legal impediment to Dade County licensing for profit, to other governmental entities, the use of any copyrighted software products which may be or have been developed by Dade County.

Jay W. Williams
Assistant County Attorney

JWW/lee